NAVAL POSTGRADUATE SCHOOL

MONTEREY, CALIFORNIA

THESIS

COMBINING FACIAL RECOGNITION, AUTOMATIC LICENSE PLATE READERS AND CLOSED-CIRCUIT TELEVISION TO CREATE AN INTERSTATE IDENTIFICATION SYSTEM FOR WANTED SUBJECTS

by

Michael J. Thomas

December 2015

Thesis Co-Advisors: Kathleen Kiernan
Patrick Miller

Reissued 3 Mar 2016 with correction to degree

THIS PAGE INTENTIONALLY LEFT BLANK

REPORT DOCUMENTATION PAGE	Form Approved OMB No. 0704–0188

1. AGENCY USE ONLY *(Leave blank)*	2. REPORT DATE	3. REPORT TYPE AND DATES COVERED
	December 2015	Master's thesis

4. TITLE AND SUBTITLE
COMBINING FACIAL RECOGNITION, AUTOMATIC LICENSE PLATE READERS AND CLOSED-CIRCUIT TELEVISION TO CREATE AN INTERSTATE IDENTIFICATION SYSTEM FOR WANTED SUBJECTS

5. FUNDING NUMBERS

6. AUTHOR(S) Michael J. Thomas

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)
Naval Postgraduate School
Monterey, CA 93943-5000

8. PERFORMING ORGANIZATION REPORT NUMBER

9. SPONSORING /MONITORING AGENCY NAME(S) AND ADDRESS(ES)
N/A

10. SPONSORING / MONITORING AGENCY REPORT NUMBER

11. SUPPLEMENTARY NOTES The views expressed in this thesis are those of the author and do not reflect the official policy or position of the Department of Defense or the U.S. Government. IRB Protocol number ____N/A____.

12a. DISTRIBUTION / AVAILABILITY STATEMENT
Approved for public release; distribution is unlimited

12b. DISTRIBUTION CODE

13. ABSTRACT (maximum 200 words)

Advancing technology in the field of facial recognition systems (FRS), closed-circuit television (CCTV) and automatic license plate readers (ALPRs) could make it possible to create a system capable of identifying suspected terrorists, current terrorist watch list suspects, other wanted criminals, and missing persons. This research examines the convergence of these technologies to design an efficient system and improve the speed and accuracy of potential suspect identification. To do so, the thesis examines all systems' basic capabilities, privacy issues or concerns, best practices, possible areas for improvement, and policy considerations.

Since the tragedies of September 11, 2001, a large volume of literature related to FRS, ALPR, and CCTV systems has been created. The intent of this thesis is to serve as catalyst for a new security system designed to locate, identify, and apprehend known terrorist watch list suspects and other wanted persons who are traversing the interstate systems in the United States. The goal is to provide another layer of protection and create a deterrent to both criminal and terrorist activity, providing a safer environment for all U.S. citizens. Furthermore, this capability can help locate Amber Alert and Silver Alert subjects.

14. SUBJECT TERMS
Facial recognition, automatic license plate readers, closed-circuit television, technology, watch list, databases, combined technologist, terrorist identification, Amber Alert, Silver Alert, interstate identification system, London City, OCR reader, photographic database, license plate database, Patriot Act, REAL ID

15. NUMBER OF PAGES
101

16. PRICE CODE

17. SECURITY CLASSIFICATION OF REPORT	18. SECURITY CLASSIFICATION OF THIS PAGE	19. SECURITY CLASSIFICATION OF ABSTRACT	20. LIMITATION OF ABSTRACT
Unclassified	Unclassified	Unclassified	UU

NSN 7540–01-280-5500
Standard Form 298 (Rev. 2–89)
Prescribed by ANSI Std. 239–18

THIS PAGE INTENTIONALLY LEFT BLANK

Approved for public release; distribution is unlimited

COMBINING FACIAL RECOGNITION, AUTOMATIC LICENSE PLATE READERS AND CLOSED-CIRCUIT TELEVISION TO CREATE AN INTERSTATE IDENTIFICATION SYSTEM FOR WANTED SUBJECTS

Michael J. Thomas
Major, Florida Highway Patrol
B.P.A., Barry University, 2006

Submitted in partial fulfillment of the
requirements for the degree of

**MASTER OF ARTS IN SECURITY STUDIES
(HOMELAND SECURITY AND DEFENSE)**

from the

**NAVAL POSTGRADUATE SCHOOL
December 2015**

Approved by: Kathleen Kiernan
Thesis Co-Advisor

Patrick Miller
Thesis Co-Advisor

Erik Dahl
Associate Chair or Instruction
Department of National Security Affairs

THIS PAGE INTENTIONALLY LEFT BLANK

ABSTRACT

Advancing technology in the field of facial recognition systems (FRS), closed-circuit television (CCTV) and automatic license plate readers (ALPRs) could make it possible to create a system capable of identifying suspected terrorists, current terrorist watch list suspects, other wanted criminals, and missing persons. This research examines the convergence of these technologies to design an efficient system and improve the speed and accuracy of potential suspect identification. To do so, the thesis examines all systems' basic capabilities, privacy issues or concerns, best practices, possible areas for improvement, and policy considerations.

Since the tragedies of September 11, 2001, a large volume of literature related to FRS, ALPR, and CCTV systems has been created. The intent of this thesis is to serve as catalyst for a new security system designed to locate, identify, and apprehend known terrorist watch list suspects and other wanted persons who are traversing the interstate systems in the United States. The goal is to provide another layer of protection and create a deterrent to both criminal and terrorist activity, providing a safer environment for all U.S. citizens. Furthermore, this capability can help locate Amber Alert and Silver Alert subjects.

THIS PAGE INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

LIST OF FIGURES

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF TABLES

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF ACRONYMS AND ABBREVIATIONS

ACLU	American Civil Liberties Union
ALPR	automatic license plate readers
BOLO	be on the lookout
CCTV	closed-circuit television
CIA	Central Intelligence Agency
DAVID	Driver and Vehicle Information Database
DHSMV	Division of Highway Safety and Motor Vehicles
EFF	Electronic Frontier Foundation
FBI	Federal Bureau of Investigation
FCIC/NCIC	Florida Crime Information Center and National Crime Information Center
FIOA	Freedom of Information Act
FRS	facial recognition system
FRVT	Face Recognition Vendor Test
IACP	International Association of Chiefs of Police
IAFIS	Integrated Automated Fingerprint Identification System
INS	Immigration and Naturalization Service
IRA	Irish Republican Army
LPR	license plate reader
MOU	memorandum of understanding
NGI	Next Generation Identification Program
NIST	National Institute of Standards and Technology
NSSE	National Special Security Events
OCR	optical character recognition
PII	personally identifiable information

THIS PAGE INTENTIONALLY LEFT BLANK

ACKNOWLEDGMENTS

I would like to take this opportunity to thank my wonderful wife, Maria, for always being there for me over the past 31 years and providing me the love, support and understanding that has allowed me to take on several challenges in life, both professional and personally. I would also like to extend thanks to my wonderful children, Nicole, Michael and Natalie, for sharing in this journey and being the rocks that hold our foundation together.

My sincere thanks to the Florida Highway Patrol and Retired Colonel David Brierton for allowing me the opportunity to attend this institution, which in turn has allowed me to gain a wealth of knowledge and understanding that I can bring back and share within our agency. Special thanks to Chief Cyrus Brown for his continued support and guidance, and for helping me gain the approval needed to attend this institution and experience a level of education that is truly astonishing.

I am extremely grateful to the Naval Postgraduate School and the Center for Homeland Defense and Security for providing me this opportunity and affording me a chance to gain valuable knowledge, which I can put to use to provide better security for those citizens under my purview.

I would like to acknowledge and thank the extraordinary cadre of NPS instructors, facilitators, staff and my two main thesis advisors, Kathleen and Patrick, for helping me make this experience so rewarding.

Finally, to the men and women of the Florida Highway Patrol who are on the front lines every day protecting and serving in an attempt to keep the public safe: I am truly grateful for your support and extremely proud of the work you do day in and day out to provide safety and security to our communities. It is an honor to serve with you, and I look forward to continuing our relationship and working hard together to provide ample security for all.

THIS PAGE INTENTIONALLY LEFT BLANK

I. INTRODUCTION

A. PROBLEM STATEMENT

Since September 11, 2001, there has been an emergence of activity surrounding terrorist groups such ISIS and Boko Haram, and the ever-present threat of Al Qaeda, along with countless homegrown terrorist groups that support their activities. These groups have increasingly called on their followers to stage attacks against the United States. Even though Timothy McVeigh and Mohammad Atta where both listed as persons of interest on the U.S. Terrorist Watchlist, they were able to avoid detection and carried out their attacks against the United States. Prior to September 11, this watch list was relatively unheard of, even though law enforcement agencies have maintained similar lists for years. The unique difference, however, between pre-9/11 watch lists maintained by individual agencies and today's Terrorist Watchlist is the cooperative sharing of information that now exists across the law enforcement community.[1] This previous lack of sharing and the ability to find suspects quickly put Americans at risk each day; *The 9/11 Commission Report* cited the lack of information sharing between intelligence collection and law enforcement agencies as a key component in the success of the World Trade Center and Pentagon attacks.[2]

If the United States is to successfully thwart future attacks, it will require a system or process that can quickly identify these suspects and lead to their apprehension at the earliest intervention opportunity. In moving forward and reviewing technology that could aid in the detection of suspected terrorist and wanted suspects—to include the combining of facial recognition systems (FRS), automatic license plate readers (ALPR), closed-circuit television (CCTV) and/or similar technology—several obstacles will have to be overcome. Some civil liberties groups may consider the convergent use of these technologies as a threat to privacy and their intentional use absent probable cause. One of

[1] Katie Rucke, "'Startling' Number of Americans are on Terrorist Watchlist," *Mint Press News*, Jully 23, 2014, http://www.mintpressnews.com/startling-number-of-americans-are-on-terrorist-watchlist/194356.

[2] Thomas Kean, *The 9/11 Commission Report: Final Report of the National Commission on Terrorist Attacks upon the United States* (Washington, DC: Government Printing Office, 2011).

the technologies these groups are concerned with is facial recognition, also known as a biometric. The term biometrics refers to "technologies that measure and analyse human physiological or behavioral characteristics for authentication or identification purposes"; biometrics often rely on identifiers such as fingerprints and voice patterns.[3]

Civil liberties groups like the Electronic Frontier Foundation and the American Civil Liberties Union (ACLU) fear that the collection of photographic images for facial recognition and other personally identifiable information (PII)—which can be collected on a subject from a distance, in open spaces, without probable cause—for people who have no connection to criminality or terrorism could be a violation of the Fourth Amendment right to privacy. These fears surround the notion that, by collecting large samplings of photographic images of a subject and his or her surroundings, one could essentially assimilate identify a person's travels, and even their religious and political affiliations, which are protected by privacy laws; however, no successful challenges have been made thus far. Since technology does have limitations, additional research would have to be conducted to determine capabilities to include strengths, weaknesses, adaptability, functionality, accuracy and feasibility to identify the best systems to meet the specific goal outlined. One other area of concern would be the capturing, sharing and retention of records associated with protected information. Policies will have to be developed that support the use of this technology and cover all issues related to its deployment, including records retention.

B. RESEARCH QUESTIONS AND CONSIDERATIONS

Can facial recognition, closed-circuit television and automatic license plate readers be combined to develop a single interstate identification system that can be used to detect suspected terrorists and wanted suspects, and/or locate missing children and elderly persons? If so, what regulatory concerns and privacy or policy considerations must be addressed for successful implementation of this system? What agencies or

[3] "Biometrics," Biometric-Solutions, accessed November 27, 2015, http://www.biometric-solutions.com/index.php.

entities would have to come together under a memorandum of understanding (MOU) or other binding construct to allow for the successful deployment of these systems?

There are currently no systems that combine these three technologies to capture watch list subjects. This thesis seeks to determine if they can, indeed, be combined into a feasible investigative tool. To do so, this research defines the minimum capabilities of FRS ALPR and CCTV, and assesses their projected capabilities as technology continues to improve. Additionally, this research evaluates existing independent policies for these technologies that may reveal a best practice scenario and guide policy for the combined technologies. This leads to an assessment of data collection and security considerations, focused on determining how the data from these systems could be collected and maintained. The research also recommends an assessment to determine if the system's anticipated added security for homeland security is worth the cost of its implementation

As noted, in developing comprehensive policy, rules and procedures for the use of these combined technologies, there must be an assurance of privacy and civil liberty protection throughout the required biometric processes (collecting, matching, storing, managing and sharing data) and the operational/business processes.[4] How should agencies develop best practices for collecting, storing and sharing images across platforms, which can include state, local, tribal, federal and commercial entities, while maintaining public trust through transparency of operations? Several civil liberties groups have already begun collecting information to challenge the legality of using this equipment, claiming that it violates a person's right to privacy. Privacy fears have often led to policies that can unintentionally or purposely hinder potentially beneficial technologies. For example, "U.S. policymakers have delayed the adoption of various public sector technologies, from smart meters to electronic identification, in part because of the pushback these technologies have received from privacy advocates."[5] In

[4] FBI, *Striking a Balance—A Government Approach to Facial Recognition Privacy and Civil Liberties* (U.S. Government Facial Recognition Legal Series Forum 2) (Washington, DC: Department of Defense, 2012).

[5] For example, activists have delayed the adoption of smart meters that measure energy usage in Nevada. See "Power Struggle: Customers vs. NV Energy Smart Meters," Fox 5 Las Vegas, February 6, 2015, http://www.fox5vegas.com/story/16689913/a-charged-debate-customers-vs-nv-energy-smart-meters.

embracing technology, however, we must also embrace changes to life patterns that the technology may bring. As humans, we tend to fear that which we do not know and accept that which is familiar. "A 'mass moral panic' occurs when one section of society distrusts or fears the choices made by others and believes these choices pose a risk to the society as a whole."[6] There must be a recognition that technology is evolving so fast that the general public and legal system may not be able to keep up; while there are no current civil actions filed, the need exists to develop and formulate policy that can withstand legal challenges and public scrutiny.

C. PRACTICAL SIGNIFICANCE OF THE RESEARCH

Surveillance systems are continually improving as technological advancements are made. Improvements can be found in technology used to distinguish one face from another (as in facial recognition), optical character recognition (OCR) readers that distinguish characters on tags in ALPRs, and CCTV systems that utilize high-definition cameras, producing images that can be imported into FRS over the Internet, or via blue tooth or WIFI connections. As these systems improve, so does their capability to scan and capture images of suspects and vehicles as they pass, allowing these samples to be analyzed against shared images in many databases, including those of state motor vehicle departments, Department of Corrections, Department of Homeland Security, Customs and Border Protection, Federal Bureau of Investigation (FBI), National Security Administration and other governmental agencies that use biometrics or house vehicle license information.

The intent of this thesis is to serve as a catalyst for the formation of a new security system designed to locate, identify and apprehend known terrorist watch list suspects and other wanted persons who are traversing the interstate systems in the United States, adding another layer of homeland security protection. These persons of interest currently move freely across the interstate system in the United States, often escaping court-ordered sanctions and allowing possible terrorist attacks against U.S. citizens or

[6] Adam Thierer, "Techno-Panic Cycles (and How the Latest Privacy Scare Fits in)," Technology Liberation Front, February 24, 2011, http://techliberation.com/2011/02/24/techno-panic-cycles-andhow-the-latest-privacy-scare-fits-in.

infrastructure. The system proposed in this thesis will also have the ability to locate Silver Alert subjects—missing elderly persons who have become disorientated and lost—and Amber Alert victims—minors who are missing or who have been abducted for nefarious purposes.

Combining FRS, ALPRs and CCTV technology will provide a system that will improve safety by creating an opportunity to identify, locate and contact persons of interest in a controlled environment outside of densely populated areas on the interstate system prior to an incident, with minimal exposure to other citizens. By design, this system becomes a force multiplier; it will create a stationary artificial means of surveillance, placing virtual eyes on the street that would improve overall U.S. security by providing a critical opportunity to detect and locate persons of interest at multiple locations without the need for on-site human presence. This will allow officers normally assigned to a fixed post to conduct roaming patrols, maximizing coverage area.

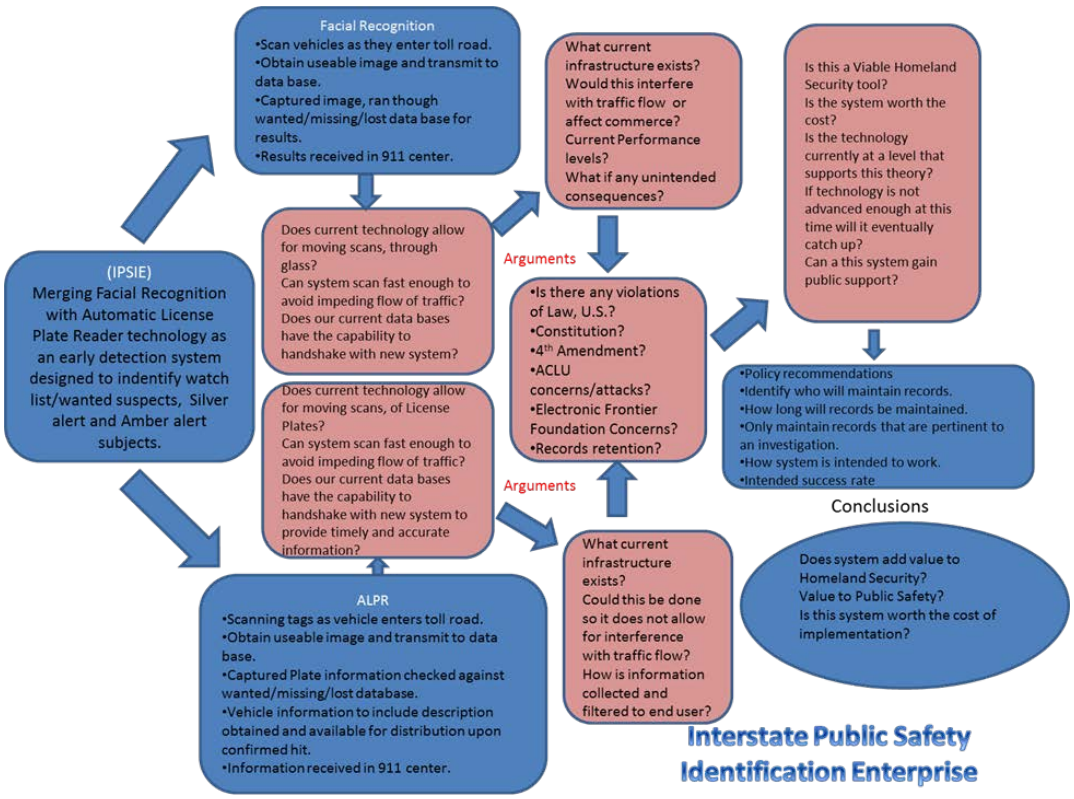
Subsequently, as these technologies become more advanced in their ability to track, identify and locate suspects, privacy concerns may intensify. This thesis conducts an in-depth review of current legal challenges, privacy concerns and court rulings related to U.S. surveillance technology. This thesis seeks to open the eyes of the public, law enforcement, judicial circuits and civil liberty groups to the feasibility of these merged technologies' possible impact on improving homeland security, while exposing the reader to legal, constitutional and regulatory challenges that may limit development and implementation. This information will allow department heads, administrators and policymakers to make informed decisions regarding how their prospective agency/entity would create policy, gain public support, develop deployment strategies, and establish records retention rules and other guidelines in support of deploying these systems.

Lastly, while this thesis attempts to mitigate possible legal challenges to privacy, the very nature of the emerging technologies and their evolution makes it difficult to forecast all future challenges, both legal and technological. Once the concept is actualized, however, it will influence industry growth and development of improved technology, resulting in increased capabilities of the proposed systems.

D. METHODOLOGY

This thesis conducted an analysis to determine if it is technically feasible and legally acceptable to combine FRS, ALPR and CCTV in order to develop a system that scans subjects and vehicles as they enter or traverse the interstate system to check against criminal, lost or wanted suspect databases. Research on the technologies was conducted to project consequences of combining these systems, along with the steps needed by law enforcement for successful adaptation and deployment of this type of system. Since these technologies have not previously been reviewed or combined, they fall into the category of emerging technologies, so research resided within the hypothetical-theoretical realm. Research was conducted utilizing a predictive mode of analysis based entirely on forecasting to determine feasibility and acceptability. The chart in Figure 1 depicts the research cycle.

Figure 1. Research Cycle



E. THESIS ORGANIZATION

The remainder of this thesis begins with an overall general discussion of technology related to personal identification through biometrics, followed by research that determines current and projected capabilities and limitations of FRS, ALPR and CCTV systems. The intent is to determine if the current technology can viably support a system designed to scan vehicles and suspects to determine if they are wanted or suspected of a crime. Once the base of the technology is discussed, analytical research (conducted to discern the technology's potential impact on homeland security and law enforcement) is described.

THIS PAGE INTENTIONALLY LEFT BLANK

II. BACKGROUND

A. FACIAL RECOGNITION

> Biometrics is often referred to the utilization of a person's physical characteristics or personal traits to that are used to identify, or verify their identity….The following represent types of biometrics that are commonly used by this approach to identify subjects; Fingerprints, faces, voices, and handwritten signatures. Biometric-based systems offer automatic, virtually immediate identification of someone by converting the biometric—a photograph, for instance—into a digital form and then analyzing it against a database housing known biometrics of an equivalent type.[7]

Facial recognition is the process of measuring an individual's overall facial structures, including the distances between their nose, mouth, eyes and jaw, and producing a mathematical value to distinctively represent and identify a face. This process is done by facial recognition software on a computer using a photograph of the subject downloaded into the system and matched against a reference photo. The quality of the reference photograph is inherently the most critical step in achieving the best possible results.

Automated face recognition was first created in the 1960s by Woody Bledsoe, Helen Chan Wolf and Charles Bisson.[8] Their program required the technician to physically "locate features such as the eyes, ears, nose, and mouth on the photograph using special mapping software."[9] The program's software then analyzed distances and ratios to a familiar reference point, comparing them to the same identifiers in the reference data.[10] Due to the extensive research of A.J. Goldstein, Leon Harmon and Ann Lesk, advancements were made in facial recognition technology that led to the development of a method that utilizes 21 specific personal markers, to include hair color,

---

[7] John D. Woodward, *Biometrics: Facing Up to Terrorism* (Santa Monica, CA: RAND, 2001).

[8] "Face Recognition Software," History of Forensic Psychology, accessed December 5, 2015, http://forensicpsych.umwblogs.org/research/criminal-justice/face-recognition-software.

[9] "Face Recognition Software," History of Forensic Psychology.

[10] National Science and Technology Council, "Face Recognition," Biometrics.gov, August 7, 2006, http://www.biometrics.gov/Documents/FaceRec.pdf.

lip thickness and other permanent facial features, to automate the recognition process.[11] This time-consuming process that used numerous intricate measurements was completely calculated, formulated and analyzed by hand.

In 1988, Michael Kirby and Lawrence Sirovich identified a procedure that "was considered a milestone because it showed that less than one hundred values were required to accurately code a suitable aligned and normalized face (void of expression). It utilized applied principle component analysis, a standard linear algebra technique, to the face recognition problem of accuracy."[12] Then, in 1991, Mathew Turk and Alex Pentland "discovered that while using the eigenfaces techniques, an appearance-based approach to face recognition that seeks to capture the variation in a collection of facial images and use this information to encode and compare images of individual faces in a holistic (as opposed to a parts-based or feature-based) manner, the residual error could then be used to detect faces in images."[13] This breakthrough allowed dependable real-time automated face recognition systems to develop. Although this new method was limited by "environmental factors, it garnered considerable interest in furthering development of automated face recognition technologies."[14] This technique sparked the reliable real-time automated facial recognition systems used today.

The first deployment of facial recognition technology that captured intense public and media attention was at the 2001 Super Bowl in Tampa, Florida. This deployment drew the attention of media and the public because it was the first time that fixed cameras would take photographs of unsuspecting visitors in an attempt to match them against a fixed database of criminal suspects. Super Bowls are considered National Special Security Events (NSSE), "as they have national or international significance deemed by the United States Department of Homeland Security…to be a potential target for

[11] A. J. Goldstein, L. D. Harmon, and A. B Lesk, "Identification of Human Faces," in *Proceedings of IEEE* 59, no. 5 (May 1971): 748–760.

[12] Lawrence Sirovich and Michael Kirby, "Low-Dimensional Procedure for the Characterization of Human Faces," *Journal of the Optical Society of America* 4, no. 3 (1987): 519–524.

[13] M. A. Turk and A. P. Pentland, "Face Recognition Using Eigenfaces," in *Proceedings of IEEE Computer Society Conference on Computer Vision and Pattern Recognition '91*, doi 10.1109/CVPR. 1991.139758.

[14] Turk and Pentland, "Face Recognition."

terrorism or other criminal activity."[15] Once a venue receives a designation of a NSSE as being a potential target of terrorism, they incur more latitude to invest in security that may uncover potential threats.

This initial usage of facial recognition software brought about a greatly needed analysis on how facial recognition systems could be deployed in an effort to support national security, while maintaining a receptive understanding of the public's concerns of social and privacy considerations.[16] The trial implementation captured surveillance images from CCTV and analyzed them across a database of digitized mug shots, discovering almost 20 fans with active arrest warrants. Since this was a large-scale test of the system designed to only test its ability to identify possible criminal suspects in large crowds, coupled with concerns surrounding the liability and accuracy of the system, no arrests were made.

The Face Recognition Vendor Test (FRVT) was performed in 2000, 2002 and 2006 with the evaluation being built upon the work of FERET (a standard dataset used for facial recognition system evaluation). In an evaluation report, it was explained that:

> The primary goals of these evaluations were to assess the capabilities of commercially available facial recognition system and to educate the public on how the facial recognition programs would properly present and analyze results.….In 2002 FRVT evaluated the progress in technology from 2000 and the performance on real-life large scale databases, and to pioneer innovative experiments to help better comprehend face recognition performance. FRVT found that given adequate controlled indoor lighting the current technology of facial recognition indicated 90% verification at a 1% false acceptance rate.[17]

Some other notable issues and discoveries include the "use of morph-able models, which maps a 2D image onto a 3D grid in an attempt to overcome lighting and pose

---

[15] Shawn Reese, *National Special Security Events* (CRS Report No. RS22754) (Washington, DC: Congressional Research Service, 2007).

[16] National Science and Technology Council, "Face Recognition," 2.

[17] Duane M. Blackburn, Mike Bone, and P. Jonathon Phillips, *Facial Recognition Vendor Test 2000: Evaluation Report* (Washington, DC: National Institute of Justice, 2001), http://www.bioconsulting.com/Facial_Recognition/FRVT_2000.pdf.

variations, can significantly improve non-frontal face recognition."[18] Additionally, watch list size will affect performance; "When comparing photographs you gain a higher level of performance using smaller databases over larger databases. Some characteristics such as age, race and sex can affect performance; some considerations should be made to include demographic information in facial recognition process."[19]

In 2006, the Face Recognition Grand Challenge "evaluated the latest face recognition algorithms available."[20] The evaluation included the use of high-resolution face images, 3D face scans, and iris images. "The results from this evaluation indicated that newer algorithms were 10 times more accurate than the face recognition algorithms of 2002 and 100 times more accurate than those of 1995…Several algorithms were able to surpass human participants in recognizing faces and could uniquely identify identical twins which had been a common error in the earlier versions."[21] This technology is rapidly evolving, furthering increasing opportunities for its deployment and use.

B. LAW ENFORCEMENT USE OF FACIAL RECOGNITION TECHNOLOGY

In late August 2001, the Central Intelligence Agency (CIA) parlayed information to Immigration and Naturalization Service (INS) officials, requesting they look out for two men alleged of terrorist activities surrounding the *USS Cole* bombing. The CIA had video of the suspects as they conversed with several others who were thought to be involved in the bombing. When the INS reviewed its database, they discovered that the two men, Khalid Almidhdhar and Nawaf Alhazmi, successfully passed through their control access points and that they had already entered the country.[22] The CIA asked the FBI to search for them, but with both individuals already in the United States, success would be difficult; they would have to search for them using traditional methods, such as visual observations, checkpoints, credit card usage checks, mobile phone traces,

[18] Blackburn, Bone, & Phillips, *Facial Recognition Vendor Test 2000*.

[19] Ibid.

[20] National Science and Technology Council, "Face Recognition."

[21] Ibid.

[22] Woodward, *Biometrics.*

informants and known associates. Alhazmi and Almidhdhar were later identified as being the two of the hijackers on American Airlines flight 77, which was deliberately crashed into the Pentagon on September 11, 2001.[23]

The use of a facial recognition programs by homeland security officials at immigration processing centers, border crossings, checkpoints, airports and ports of entry may help locate or capture known or suspected terrorists or deter them from entering the United States. Sharing this information with homeland security partners, including law enforcement, will provide increased opportunities to locate suspected terrorist or watch list suspects, both strategically—as they attempt to enter the United States—and by happenstance—after they have already crossed the border, if any should come into a chance meeting with law enforcement authorities. It is unknown if the use of a FRS could have stopped the events of September 11, 2001, since the technology was not fully developed and used in that capacity at that time. In looking forward, law enforcement agencies must continue to develop current technologies and invest in future technologies in an effort to thwart terrorist events.

Learning from federal applications, in 2001, the Pinellas Sheriff's Office in Florida began implementing a facial recognition program called the Face Analysis, Comparison, and Examination System (FACES). The program started out with the collection of booking photographs from the Pinellas County Jail and Florida's Department of Correction's database. In 2011, Pinellas County was able to tap into Florida's Department of Highway Safety and Motor Vehicles (DHSMV), Driver and Vehicle Information Database (DAVID) and 36 partner agencies within the state. The DAVID database contains the records of all Florida's licensed drivers, to include all vehicles owned and registered by the driver, and his or her current address, contact information for emergency notifications and a facial-recognition quality digital photo image and signature of the licensee.[24] As a division of the DHSMV, the Highway Patrol has had an opportunity to work closely with the Pinellas County Sherriff's Office during

[23] Terry McDermott, *Perfect Soldiers: The Hijackers: Who They Were, Why They Did It* (New York: Harper Collins, 2005), 330.

[24] Florida Highway Safety and Motor Vehicles, "DAVID—Law Enforcement's Best Information Tool," *Legal Highway* III, no. 1 (Spring/Summer, 2013): 1.

all phases of their program's development in regards to data collection, sharing and retention.

The Pinellas County Sherriff's Office is notably one of the first law enforcement agencies to implement use of facial recognition technology. It is speculated that they currently have the largest photo data base of any law enforcement agency in the country.[25] Several agencies in Florida and around the nation have been working on facial recognition for several years, and it has already been used for large events such as the 2011 Super Bowl in Tampa and, most recently, following the Boston Marathon Bombing. Cities across America have been installing cameras in open areas, areas of commerce and high-crime locations; given the quality of the images collected, they could be used to capture photographs for facial recognition.[26]

C. CLOSED-CIRCUIT TELEVISION (CCTV)

CCTV was developed by Walter Brunch, a German engineer who was attempting to watch the launch of two rockets simultaneously in 1942.[27] In the mid-1960s, Marie Brittian Brown was the first to use CCTV as a security system. Brown created the system after noticing that law enforcement officers had lengthy delays in their response to calls. In her exploration to discover a new method to provide increased safety for homes more effectively, she had the idea "to use cameras and a TV to solve the problem."[28] Since their inception, CCTV systems have evolved immensely and are now, thanks to technological advancements, are now only a shadow of the first designs. This section examines how CCTV has evolved in both the United Kingdom and the United States.

---

[25] Jacob Ruberto, "Interagency use of Facial Recognition" (Atlanta, GA: Pinellas Sheriff's Office, 2013).

[26] Ruberto, "Interagency Use of Facial Recognition"; Joshua C. Klontz and Anil K. Jain, *A Case Study on Unconstrained Facial Recognition Using the Boston Marathon Bombings Suspects* (Tech. Rep. MSU-CSE-13-4) (Lansing, MI: Michigan State University, 2013).

[27] Marshall Jones Jr., "Who Invented the First CCTV System?" Sonitrol, June 30, 2015, http://www.sonitrolky.com/invented-first-cctv-system/.

[28] Jones, "Who Invented the First CCTV System?"

1. United Kingdom CCTV Model

Great Britain's use of CCTV is recognized as one of the most expansive. It was first used in 1961 in a London train station, where surveillance cameras were placed in public areas to provide security to citizens.[29] Initially created to identify and combat criminal activity on and around mass transit systems, the systems have prevailed for years and have evolved over time to combat terrorist activity.[30] In 1993, the Irish Republican Army (IRA) carried out an attack at Bishop Gate in Central London. This attack was the catalyst that moved the United Kingdom toward developing and initiating enhanced CCTV strategies.[31] The objective was to create a system that would allow the British government to uncover suspected IRA activity in the planning stages before an actual attack.[32] The attack eventually led to the development of the "ring of steel" in August of 1993. The ring of steel surrounds the City of London, also known as "Central London," which encompasses approximately one square mile and contains an estimated 450 cameras in 230 different positions.[33] Central London officials made a strategic move to limit the entry points into the area by blocking off several roads, and created choke points by placing barriers and speed humps, which intentionally slowed the vehicles down to allow for a more accurate capture of their license plate and a clear photograph of the driver. These cameras were later integrated into vehicle registration data bases, which allowed the tags of all vehicles entering the area to be checked.

Another significant event that shaped the Great Britain's use of CCTV was the February 12, 1993 abduction and brutal killing of a child named James Bulger. The abduction and killing, along with the assailants—two 10 years old boys—were captured

---

[29] "The History of CCTV in the UK" SRMTI, accessed November 27, 2015, http://www.srmti.com/news/the-history-of-cctv-in-the-uk-10079/.

[30] Michael McCahill and Clive Norris, *CCTV Systems in London: Their Structure and Practices* (Working Paper No. 10) (Hull, UK: University of Hull, 2003).

[31] McCahill and Norris, *CCTV Systems in London*, 2.

[32] Nils Zurawski, "I Know Where You Live! Aspects of Watching, Surveillance and Social Control in a Conflict Zone," *Surveillance & Society* (2005): 508.

[33] Jon Coaffee, "Rings of Steel, Rings of Concrete and Rings of Confidence: Designing out Terrorism in Central London Pre- and Post-September 11th," *International Journal of Urban and Regional Research* 28, no. 1 (2004): 201–211.

on a shopping mall's CCTV system.[34] This heinous crime demonstrated the need for surveillance feeds to be monitored in person. There are an estimated 4.2 million surveillance cameras currently monitoring the United Kingdom.[35] London has a far greater estimated number of surveillance systems currently monitoring their citizens within the confined area of London Central than do most U.S. cities. Beijing, London, Chicago, Houston, and New York are considered the top-five world cities that utilize CCTV systems (see Figure 2 for a more precise breakdown).[36]

Figure 2. Worldwide CCTV Systems Ranking

Location	Number of Cameras	Notes
United Kingdom	1.85 Million	1 camera for every 14 people
Beijing	470,000	70,000 added since 2010
City of London	420,000	
Chicago	17,000	
Houston	Exact number not released to the public	2.3 Million Population
New York	4,450	Mostly owned by private companies

Adapted from "Top 5 Cities with the Largest Surveillance Camera Networks," VinTech, May 4, 2011, http://www.vintechnology.com/journal/uncategorized/top-5-cities-with-the-largest-surveillance-camera-networks/.

[34] Tom Sharratt, "James Bulger 'Battered with Bricks,'" *Guardian*, 1993.

[35] Tom Reeve, "How Many Cameras in the UK? Only 1.85 Million, Claims ACPO Lead on CCTV," Security News Desk, March 2011.

[36] "Top 5 Cities with the Largest Surveillance Camera Networks," VinTech, May 4, 2011, http://www.vintechnology.com/journal/uncategorized/top-5-cities-with-the-largest-surveillance-camera-networks/.

In the 1990s, the United Kingdom made the expansion of CCTV a priority, spending over 78 percent of the government's crime prevention funds on improving and increasing CCTV systems.[37] In the United Kingdom, the government body that is tasked with providing oversight to the CCTV program is called the Home Office. The Home Office, which is similar to the United States' Department of Homeland Security, establishes policy and best practices, providing oversight of CCTV programs; this includes identifying stakeholders and providing an understanding of their roles to municipalities, who then manage the systems.[38] The Home Office is also responsible for homeland security, immigration, law and order, maintaining oversight of police, visas and the security service known as MI5. These responsibilities also extend to governmental policy in several areas relating to its mission to include ID cards, drugs and counter-terrorism.

An estimated 40 percent of open, public space in the United Kingdom is blanketed by CCTV systems, which is significantly higher than other counties, likely due to privacy concerns.[39] These systems, both private and public, are centrally regulated and controlled by the 1998 Data Protection Act, which regulates collection, storage and licensing of all security personnel responsible for operating these systems.[40] It requires that entities that employ these types of systems, to include CCTV, notify the Information Commissioner. "When registering a system the user must state what the purpose of a system is, and once registered compliance with a number of legally enforceable principles is required, including adoption of a suitable code of practice."[41] In accordance, the British data commissioner issued a document called the "CCTV Codes of Practice,"

---

[37] Kristie Ball et al., *A Report on the Surveillance Society* (United Kingdom: Surveillance Studies Network, 2006), https://www.priv.gc.ca/information/int/2006/surveillance_society_full_report_2006_e.pdf.

[38] Home Office, *Surveillance Camera Code of Practice* (London: The Stationary Office, 2013), https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/204775/Surveillance_Camera_Code_of_Practice_WEB.pdf.

[39] Leon Hempel and Eric Topfer, *CCTV in Europe: Final Report* (Working Paper No. 15) (Berlin: Technical University Berlin, 2004), http://www.urbaneye.net/results/ue_wp15.pdf.

[40] "Data Protection Act 1998," The National Archives, accessed December 17, 2015, http://www.legislation.gov.uk/ukpga/1998/29/contents.

[41] Marianne L. Gras, "The Legal Regulation of CCTV in Europe," *Surveillance & Society* 2, no. 2/3 (2002).

which outlines general rules for the use of CCTV systems. These rules govern data protection, storage and image use, and require that every CCTV system is registered with the government to verify compliance with these guidelines.[42] In addition to this legislation, CCTV is also monitored by the 1998 Human Rights Act, and the 1998 Crime and Disorder Act.

The United Kingdom employs the philosophy that security is everyone's responsibility and, to that end, has gained a large volume of public support. Britain's CCTV system relies heavily on partnerships with the private industry, local community and law enforcement, who work together to create a cohesive security system. The strength of these local partnerships is attributed to British citizens' support and acceptance of a society under constant surveillance. Another key factor that lends to this acceptance is that the Home Office, which is deemed a separate entity, provides oversight to "law enforcement and domestic intelligence-gathering agencies that have access to the surveillance systems."[43] The second layer of protection is the formulation of the Data Protection Act which, in Britain, outlines the guidelines, procedures, roles and legal constraints to be adhered to by the Home Office and individual municipalities that administer the cameras.[44] There are currently no rules governing how private partners, to include homeowners and local business owners, use CCTV cameras. It is generally assumed that an attempt to regulate these cameras would face strong opposition, as citizens believe they provide personal security and are an important part of crime prevention.

Studies on the efficiency of CCTV are varied; in most cases, however, vehicle crimes, burglary and theft appear to decrease in areas with CCTVV systems. CCTV systems report a smaller decrease in deterring crimes against persons (battery, assault, domestic violence), which could be a result of those crimes being emotional and personal in nature. Most of the studies do indicate that CCTV systems are successful in deterring crime in coverage areas. This, however, creates the unintended consequence of

[42] Gras, "The Legal Regulation of CCTV in Europe."

[43] Home Office, *Surveillance Camera Code of Practice*.

[44] Act, Data Protection, *UK Parliament* (1998)

displacement, which causes criminals to commit crimes in areas known to not be covered by CCTV systems.[45]

2. The United States' Use of CCTV

Prior to the attacks on September 11, 2001, some U.S. cities experimented with CCTV systems, including New York City; Virginia Beach, Virginia; and Tampa, Florida. In 1993, New York City placed cameras in its transit system to deter crime. Unfortunately, the program was stopped in 1985 after it was deemed unsuccessful.[46] Similar attempts were made by Virginia Beach in 2002 and Tampa in 2001. Not only did these two cities utilize CCTV, they also merged facial recognition technology to explore its effectiveness. They, too, suffered some of the same criticism, with experts indicating that the results were inconclusive.[47]

Following the attacks on September 11, cities and law enforcement agencies across the United States began searching for new strategies and technologies to instill a sense of safety and security. Several cities across the United States have been attempting to develop and implement CCTV programs to provide surveillance in high-risk crime areas, such as downtowns and commercial districts. One of the first large-scale implementations of CCTV technology was in Washington, DC, by the Metropolitan Police Department soon after the September 11 attacks.[48] The system was designed to sustain public safety operations in the nation's capital throughout major events, emergencies, or when the nation is on high alert for possible terrorist attacks. The system only monitors public spaces, with special attention given to critical installations that officials have branded probable terrorism targets.[49]

---

[45] Rachel Armitage, "To CCTV or Not to CCTV: A Review of Current Research into the Effectiveness of CCTV Systems in Reducing Crime," Nacro, May 2002, https://epic.org/privacy/surveillance/spotlight/0505/nacro02.pdf.

[46] Deirdre Carmondy, "Subway Anticrime TV Test Abandoned." *New York Times,* August 4, 1985.

[47] "Va., Beach Police End Failed Facial Recognition Program," *Richmond Times-Dispatch,* August 28, 2007.

[48] "MPDC's Closed Circuit Television (CCTV) System," MPDC, accessed May 27, 2015, http://mpdc.dc.gov/page/mpdcs-closed-circuit-television-cctv-system.

[49] "MPDC's Closed Circuit Television (CCTV) System."

Following DC's lead, several other cities, including Houston, New York, Chicago, Baltimore, Newark and Charleston, have joined the ranks in adding CCTV surveillance systems. A 2007 report by the ACLU (located in Northern California) cited some 37 California cities that had implemented CCTV programs.[50] NYPD currently uses a CCTV system to conduct surveillance of Midtown Manhattan, the financial district and other strategic locations designed to protect critical infrastructure, with no legal challenges to date. Several Department of Corrections facilities have also deployed CCTV systems and have sparked little or no controversy.[51] The International Association of the Chiefs of Police conducted a survey that revealed 80 percent of responding police agencies are currently utilizing some form of CCTV.[52] The most common uses for CCTV by police are in car videos, interrogations rooms and ingress and egress into governmental buildings. Law enforcement officials in the United States have been reasonably successful in obtaining videos from private owners and businesses upon request when conducting criminal investigations. However, due to the lack of mandatory regulation identifying retention lengths, there have been instances in which videos have been erased or overwritten. Most of the video surveillance systems throughout the United States are controlled by municipalities through public and private partnerships.

The United States' biggest failing thus far in their use of CCTV systems is the lack of sufficient manpower to monitor cameras twenty-four hours a day (control centers). Most U.S. systems have attempted to mirror the U.K. system; however, so far, studies regarding the effectiveness of the systems for crime prevention have been inconclusive.[53] In contrast to the U.K. system, the use of CCTV has not been widely accepted by the public. In order to have successful deployment of this system, public, legislative, and government official support and buy-in will be paramount.

---

[50] Mark Schlosberg and N. Ozer, *Under the Watchful Eye: The Proliferation of Video Surveillance Systems in California* (New York: American Civil Liberties Union, 2007).

[51] Jolene Hernon, "CCTV: Constant Cameras Track Violators," *NIJ Journal*, no. 249 (2003): 16–23.

[52] Laura J. Nichols, *The Use of CCTV/Video Cameras in Law Enforcement* (Alexandria, VA: International Association of Chiefs of Police, March 2001), Executive Summary.

[53] Rajiv Shah and Jeremy Braithwaite, "Spread Too Thin: Analyzing the Effectiveness of the Chicago Camera Network on Crime," *Police Practice and Research* 14, no. 5 (2013): 415–427.

D. AUTOMATED LICENSE PLATE READER (ALPR) TECHNOLOGY

In 1976, the Police Scientific Development Branch invented (in the U.K.'s Home Office), invented ALPR technology.[54] License plate reader systems consist of "high-speed cameras combined with sophisticated computer algorithms capable of converting the images of license plates into computer-readable data."[55] According to Roberts and Casanova, license plate reader (LPR) systems

> typically utilize specialized cameras designed to capture images of license plates, whether from fixed positions or mobile patrol vehicles. Images of vehicles and license plates are the primary form of information collected by a LPR system. Optical character recognition ("OCR") is performed on these images and the alphanumeric characters on each license plate are rendered into an electronically readable format. LPR systems can attach date, time, and location information to an image. A license plate number does not identify a specific person; rather it simply identifies a specific vehicle.[56]

The LPR system was primarily designed to detect stolen vehicles and license plates; some applications, however, allow for cameras to be set in stationary locations around a city, especially in high-crime areas, collecting license plate data for all vehicles entering and leaving the area.[57] If a crime occurs in this area, the system would allow agencies to mine the databases in order to determine what vehicles were in the vicinity of the crime scene and provide photos of those vehicles to investigators. The owners could then be located and interviewed.

---

[54] Many references indicate that Police Scientific Development Branch developed ANPR in 1976 (see, e.g., Ch. Jaya Lakshmi, A. Jhansi Rani, K. Sri Ramakrishna, and M. KatiKiran, "A Novel Approach for Indian License Plate Recognition System," *International Journal of Advanced Engineering Sciences and Technologies*, 6(2011): 10–14.

[55] IACP, *Privacy Impact Assessment Report for the Utilization of License Plate Readers* (Alexandria, VA: International Association of Chiefs of Police, 2009).

[56] David J. Roberts and Meghann Casanova, *Automated License Plate Recognition (ALPR) Systems: Policy and Operational Guidance for Law Enforcement* (Washington, DC: National Institute of Justice, 2012).

[57] Cynthia Lum, Linda Merola, Julie Willis, and Breanne Cave, *License Plate Recognition Technology (LPR):Impact Evaluation and Community Assessment* (Fairfax, VA: George Mason University, 2010); Roberts and Casanova, *Automated License Plate Recognition.*

E. LEGAL CHALLENGES FOR FACIAL RECOGNITION

As facial recognition technology improves, increasing law enforcement and commercial industry use, several civil liberty groups have raised concerns pertaining to "individual privacy." Today, cameras are considered a way of life. Photos are collected everywhere from traffic lights and cell phones to home security and corporate security systems. Photos are rapidly copied and downloaded from social networking sites or other online forums. All these photographs could eventually be used in conjunction with facial recognition programs.[58] Currently, in the United States, there are no laws that prohibit the use of facial recognition; however, some have questioned if this technology infringes a right to privacy, based on their interpretation of the language outlined in the U.S. Constitution. Civil liberty groups citing the Fourth Amendment are actively collecting information in preparation for court challenges. Most of these privacy arguments are loosely based on several provisions in the Bill of Rights, highlighted during the Supreme Court ruling of Whalen v. Roe, which reiterated that the "right to privacy is one of the most fundamental constitutional rights."[59]

The civil liberties group Electronic Frontier Foundation (EFF) has expressed concerns over the FBI Next Generation Identification (NGI) Program and its attack on individual privacy. NGI is being developed to replace/build upon the current Integrated Automated Fingerprint Identification System (IAFIS), and involves the collection and storage of biometrics to include digital photographs, fingerprints, iris scans and palm prints. The FBI's IAFIS "fingerprint database already contains well over 100 million individual records, equal to nearly one third of the U.S. population."[60] In 2013, the NGI database contained over 16 million photographs, with an estimated increase in collection and storage of photographs to 52 million by 2015.[61] The EFF is concerned that, in this

---

[58] J. Meek, "Robo Cop: Some of Britain's 2.5 Million CCTV Cameras Are Being Hooked up to a Facial Recognition System Designed to Identify Known Criminals," *Guardian*, 2002.

[59] *Whalen v. Roe*, 429 U.S. 589, 97 S. Ct. 869, 51 L. Ed. 2d 64 (1977).

[60] Jennifer Lynch, "FBI Plans to Have 52 Million Photos in its NGI Face Recognition Database by Next Year," Electronic Frontier Foundation, April 14, 2014, https://www.eff.org/deeplinks/2014/04/fbi-plans-have-52-million-photos-its-ngi-face-recognition-database-next-year.

[61] Lynch, "FBI Plans."

system, images of non-criminals will be stored alongside criminals. The FBI has indicated that, among the photographs contained in the NGI database, approximately 4.3 million are of non-criminal offenders obtained for noncriminal purposes, such as employer background checks.[62]

The FBI claims the database will "reduce terrorist and criminal activities by improving and expanding biometric identification and criminal history information services through research, evaluation and implementation of advanced technology within the IAFIS environment."[63] The ACLU, however, has expressed concerns regarding facial recognition, fearing First Amendment violations, as mentioned in Chapter I.[64] The EFF argues that if biometric data using technology is to be used, it should only be used on subjects convicted of a crimes, not all citizens who have active driver's licenses or passports.[65] The EFF's argument might be a moot point, however, as the FBI has not provided the public with the procedures that will be used to facilitate facial recognition analysis across different platforms to federal, state, local and tribal actors. Despite early statements from the FBI to the media that NGI will merely be a mugshot database, "the Bureau's plans for its face recognition capabilities are much broader….According to an FBI presentation on facial recognition and identification initiatives at a biometrics conference in 2010…one of the FBI's goals for NGI is to be able to track people as they move from one location to another."[66]

Several arguments have been raised concerning the use of facial recognition in open spaces, as it does not afford the subject it is scanning to know the process is

---

[62] Lynch, "FBI Plans."

[63] "Privacy Fears over FBI Facial Recognition Database," BBC, April 15, 2014, http://www.bbc.com/news/technology-27037009; "FBI Introduces Next Generation Facial Recognition Technology," Death and Taxes, October 20, 2011, http://www.deathandtaxesmag.com/152857/fbi-introduces-next-generation-facial-recognition-technology/.

[64] Claire Guthrie Gastañaga, "Protecting Privacy while Keeping Us Safe: Technology and Liberty," ACLU, June 4, 2014, http://acluva.org/15321/protecting-privacy-while-keeping-us-safe-technology-and-liberty/.

[65] Lynch, "FBI Plans."

[66] Richard W. Vorder Bruegge, "Facial Recognition and Identification Initiatives," FBI, 2010, http://biometrics.org/bc2010/presentations/DOJ/vorder_bruegge-Facial-Recognition-and-Identification-Initiatives.pdf.

occurring. Opposition groups have implied that this constitutes an unreasonable search, violating a person's right to move around freely and, consequently, the Fourth Amendment.[67] These arguments have not been successfully challenged in the legal system to date, although the ACLU has requested information from agencies utilizing these systems for possible challenges. Raffie Beroukhim, vice president of the NEC Corporation of America, Biometrics Solutions Division, explains that "facial recognition remains a major focus of forensic research because of its non-invasive nature and because it is people's primary method of person identification."[68]

Law enforcement officials have been turning to social media sites such as Google+, Facebook and Twitter to collect and compare photographs of suspected criminals, known criminals or missing persons; Facebook reports to have 250 billion photographs, in comparison with the FBI's estimated 50 million.[69] This effort has shown significant success and has led to the arrest of several criminals wanted for various crimes. Facebook uses facial recognition technology to automatically tag a Facebook user in a photograph by comparing the new photograph to others already online, a process that takes only a few seconds. Facebook's success in facial recognition comes from its ability to analyze photographs that are considered ideal as the system can scan the volume of photographs submitted by each subject, finding the photograph with the optimum angle, lighting, contrast and clarity.[70] In March 2012, the New York Police Department caught 37-year-old shooting suspect Jordan Rodriquez in Queens after finding his nickname, searching social media sites for a photograph and running through their facial recognition software.[71]

---

[67] Jack Carey, "ACLU Protests High-Tech Super Bowl Surveillance," *USA Today*, February 6, 2002, 2002.

[68] John Dowden, "Facial Recognition: The Most 'Natural' Forensic Technology," *Evidence Technology Magazine* 11, no. 5 (September–October, 2013), http://www.evidencemagazine.com/index.php?option=com_content&task=view&id=1344.

[69] Brandon Russell, "Why Facebook is Beating the FBI at Facial Recognition," The Verge, July 7, 2014, http://www.theverge.com/2014/7/7/5878069/why-facebook-is-beating-the-fbi-at-facial-recognition.

[70] Russell, "Why Facebook Is Beating the FBI."

[71] Jim Watson, "NYPD Uses Facebook and Facial Recognition Program to Arrest Suspect," RT, March 19, 2012, https://www.rt.com/usa/new-york-barbershop-shooting-951/.

In response to corporate America utilizing facial recognition applications, U.S. Senator Al Franken (a Democrat from Minnesota and chairman of the Senate Subcommittee on Privacy, Technology and the Law) has expressed serious privacy concerns about applications that give strangers personal information, including a person's name, photographs and dating website profiles. Senator Franken asked that makers of these applications limit the facial recognition feature to only those people who have given prior consent, noting that these types of applications raise serious concerns for personal safety and individual privacy.[72]

Concerns have also been lobbied that law enforcement agencies are not only scanning for wanted subjects; they are also collecting a database of photographs that could be used later within the system.[73] A second concern is that these photos could be used to track an innocent person's movement, as most photographs are now embedded with GPS coordinates and date/time stamps.[74] These concerns are not valid currently, as most of the photographs the department will utilize have come from stationary locations, such as a county jail upon a subject's incarceration or a driver's license office. As this system evolves and the uses of other photographs are routinely filtered into the system, this may be a topic to revisit.

F. LEGAL CHALLENGES FOR AUTOMATIC LICENSE PLATE READERS (ALPRS)

ALPR use has faced challenges similar to FRS use from civil liberty groups. In identifying possible privacy issues and developing policy to effectively implement a system combining both technologies, it is imperative to address these concerns in the implementation stage to mitigate possible challenges.

The ACLU is concerned that ALPRs indiscriminately track the location of drivers and their movements, embedding GPS locations and date and time stamps, which

---

[72] "Sen. Franken Raises Concerns about Facial Recognition App that Lets Strangers Secretly Identify People," Al Franken Senator for Minnesota, February 5, 2014, http://www.franken.senate.gov/?p=press_release&id=2699.

[73] "Privacy Fears," BBC.

[74] Gastañaga, "Protecting Privacy."

infringes on individual privacy.[75] Similar concerns relate to the storage of LPR data, as the system records every license plate, regardless of its connection to a crime. The challenge would be creating a system that removes plate data that is not associated with a specific crime after it is determined that the data is no longer viable for an investigation. "The spread of these scanners is creating what are, in effect, government location tracking systems recording the movements of many millions of innocent Americans in huge databases," said ACLU Staff Attorney Catherine Crump.[76] The ACLU has expressed the same concerns recently over facial recognition programs across the nation.

Another issue surrounding the ALPRs pertains to record retention. In late 2013, the Boston Police Department suspended their LPR system following an information leak that "inadvertently released the license plate numbers of more than 68,000 vehicles" that had tripped alarms on ALPRs over a six-month period to a media outlet.[77] Currently, New Hampshire is the only state that has passed legislation that forbids the use of license plate readers. Over 38 state police agencies and 70 percent of all other law enforcement agencies in the U.S. are currently using LPR systems, with all of them having different retention length requirements for the information collected. In Utah, the police are required "to delete license plate data nine months after collection."[78] "In Vermont the limit is 18 months and in Maine it is three weeks."[79] Arkansas police have to throw out the plate numbers after 150 days, and some agencies have no rule or law preventing them from housing the information indefinitely. In preparation of challenges to safeguarding

---

[75] "You Are Being Tracked: How License Plate Readers Are Being Used to Record Americans' Movements," ACLU, accessed July 26, 2014, https://www.aclu.org/technology-and-liberty/you-are-being-tracked-how-license-plate-readers-are-being-used-record.

[76] "ACLU Releases Documents on License Plate Scanners from some 300 Police Departments Nationwide," ACLU, July 17, 2013, https://www.aclu.org/technology-and-liberty/aclu-releases-documents-license-plate-scanners-some-300-police-departments.

[77] Shawn Musgrave, "Boston Police Halt License Plate Scanning Program," *Boston Globe*, December 14, 2013.

[78] B. Shockley, "Lawsuit Challenges State of Utah Ban on License Plate Readers," Vigilant Solutions, February 13, 2014, http://vigilantsolutions.com/press/drn_vigilant_utah_lpr_federal_lawsuit.

[79] "Automated License Plate Readers, State Statutes Regulating Their Use," National Conference of State Legislatures, February 2, 2015, http://www.ncsl.org/research/telecommunications-and-information-technology/state-statutes-regulating-the-use-of-automated-license-plade-readers-alpr-or-alpr-data.aspx.

information in relation to photographs stored in agencies data bases, agencies will need to build in acceptable retention lengths during the implementation stage.

G. PUBLIC ACCEPTANCE AND CCTV

Public Acceptance is critical in developing and implementing a successful CCTV system. Several studies have been conducted on CCTV usage in the United Kingdom and the early reports indicated that that only a small percentage of citizens were concerned about the government surveillance systems infringing civil liberties. A mid-1990s "Glasgow poll showed a 95 percent acceptance rate for public surveillance systems."[80] Recent surveys in the United Kingdom consistently show an acceptance rate of more than 65 percent.[81] Regarding civil liberties abuses, however, the public held a relatively low concern, in the 12–19 percent range.[82] In stark contrast to the public acceptance enjoyed by the United Kingdom, an American poll "showed that only 40% of Americans supported more cameras in the name of public safety—and only 12% wanted fewer cameras"; however, several planned programs have been put on hold due to privacy fears.[83]

H. TECHNICAL CONCERNS

Facial recognition is still in its infancy as far as technology is concerned; even though it shows promise, it is still limited by several factors. Most of the issues surrounding the proposed system are centered on the quality of the photograph used for analysis. In some instances poor camera angle, limited lighting, skewed facial expressions, shadowing and other parameters, can significantly impact the systems capability to recognize target subjects.[84] Photographic quality not only pertains to the photograph sample taken of a subject during a law enforcement encounter, surveillance

---

[80] P. Edwards and N. Tilley, *CCTV–Looking Out for You* (London: Home Office, 1994).

[81] Michael McCahill and Clive Norris, *CCTV in Britain* (Working Paper No. 3) (Berlin: Technical University Berlin, 2002).

[82] Martin Gill and Angela Spriggs, *Assessing the Impact of CCTV* (London: Home Office Research, Development and Statistics Directorate, 2005).

[83] Kate Dailey, "The Rise of CCTV Surveillance in the US," *BCC News Magazine*, April 29, 2013.

[84] Woodward, *Biometrics.*

camera, red light camera or downloaded from a social network site, it also encompasses the photograph stored in one of the many databases that will be drawn upon for comparison. Recent facial recognition systems have demonstrated that they can be quite accurate and produce fast results, provided they have quality samples. The U.S. National Institute of Standards and Technology (NITS) conducted several evaluations on facial recognition systems in 2010, leading them to the discovery that the best algorithms correctly recognized "92 percent of unknown persons from a database comprised of 1.6 million criminal records."[85] With technical advancements, these systems will continue to experience better their rapid detection and ability to build a full facial image from only small particles of data. The increased interest in facial recognition technology, as well as advancements with general camera systems that allow for higher-resolution photographs from all sources, will allow facial recognition photo databases to increase dramatically. The only real foreseen obstacle will be processor speeds, which will need to be high in order to sort through databases and identify wanted suspects in a timely manner.

In recognizing the need for information security, all sharing of information across platforms with other law enforcement entities will require acknowledgment of a memorandum of understanding (MOU).[86] In moving forward with its use of facial recognition, the Florida Highway Patrol Policy and Accreditation Division researched legislation, legal opinions and best practices of other agencies, and has found little in relation to issues concerning facial recognition. The International Association of Chiefs of Police (IACP) currently has no guidelines or policy recommendation on the use of facial recognition. Florida Highway Patrol should place emphasis on information security with the development of facial recognition program policies and practices. This policy will mirror practices already deployed in other applications in which security is critical. In an effort to safeguard sensitive information, all data will be marked law enforcement sensitive and only accessed for law enforcement use.

---

[85] Patrick J. Grother, George W. Quinn, and P. Jonathon Phillips, *Report on the Evaluation of 2D Still-Image Face Recognition Algorithms* (NIST Interagency Report 7709) (Gaithersburg, MD: NIST, 2010), 106.

[86] Yue Liu, "Biometrics and Privacy Protection in USA's Constitution," *International Journal of Private Law* 4, no. 1/2110 (January, 2011): 54–68.

This technology could one day allow law enforcement to scan traffic violators and civilians in public areas such as parking lots, fast food restaurants and other locations without their knowledge. These scans will concurrently check them against the states driver's license database local jail booking photographs and potentially the FBI's facial recognition database. FHP is in the process of working with the FBI to formulate an information sharing connection that would also allow us to tap into their data bases for cross referencing (see Appendix A).[87] The unique aspect of the FBI's data base is that each photograph will be attached to subjects fingerprint data for cross referencing. This is a direct result of the Patriot Act, which are intended to create an accurate identification process.

I. NOTABLE SUCCESSES

A recent successful deployment of facial recognition technology includes Nevada's Department of Motor Vehicle's fraud investigation unit, formed in 2003 in response to the attacks of September 11, 2001; using computerized facial recognition technology, this unit has successfully caught eight to ten people a day attempting to obtain fake driver's licenses. Some are teenagers seeking fake IDs to gain access to bars and clubs. Of the remaining outliers, some were discovered to be illegal immigrants attempting to obtain false identifications to pose as U.S. citizens to avoid deportation, others were felons trying to conceal prior criminal activity, and some were subjects attempting to gain a false identification to allow them to commit new crimes under assumed identities.[88]

In March 2014, facial recognition software in Florida nabbed a killer who escaped from prison in 1977. Convicted killer James Robert Jones, living under the assumed name of Bruce Walter Keith, was married and working for an air conditioning company until his capture. Jones was listed as one of the Army's 15 most-wanted fugitives after he escaped from the Kansas prison known as the Castle for its large walls and tower keeps.

---

[87] See Appendix for sample of FBIMOU Interstate Photo System Facial Recognition Pilot, provided by Jennifer Lynch (Electronic Frontier Foundation), September 2, 2014.

[88] Abigail Goldman, "DMV Making Identity Thieves' Faces their Own Worst Enemies," *Las Vegas Sun*, August 26, 2009.

U.S. Marshals caught up to Jones after facial recognition technology matched a Florida driver's license he was issued in 1981 in Bruce Keith's name with his prior military identification photo.[89]

Federal facial recognition technology also led to the capture of a fugitive from justice that was on the run for 14 years. Neil Stammer fled the United States in 1999 after he was arrested for kidnapping and child sex abuse. In January 2014, an agent with the U.S. Diplomatic Security Service, which protects, U.S. embassies and monitors visa and passport use, tested the service's new facial recognition technology by comparing current passport photos with the FBI's online wanted posted database. The system, which is designed to catch passport fraud, matched an updated photo of Stammer from the FBI's Albuquerque division to a passport photo tied to a different name. Following the discovery, authorities captured Stammer in Nepal and extradited him to the United States.[90]

The charts in Tables 1, 2, and 3 contain historical data for calls received by the Florida Highway Patrol and dispatched to officers on patrol to locate persons of interest. This data compares the number of calls reported and subjects located with the number of subjects not located in relation to "be on the look-out" (BOLO) calls for known wanted suspects, Silver Alert subjects (missing elderly subjects) and Amber Alert subjects (missing or abducted children) maintained by the Florida Highway Patrol Business Analyst Section for the five-year period of January 1, 2010 through October 1, 2015.[91]

---

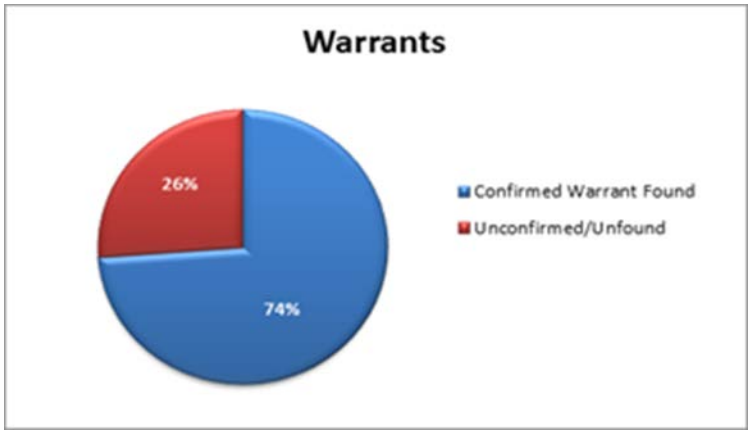
[89] "Facial Recognition Software Nabs Killer Who Escaped from Prison in 1977," *Tulsa World*, March 14, 2014.

[90] Giuseppe Macri, "FBI and Government Facial Recognition Tech Catch Fugitive on the Run for 14 Years," *Daily Caller*, August 13, 2014.

[91] Brooke Powell (Florida Highway Patrol Business Analyst Supervisor), in discussion with the author, October 8, 2015.

Table 1. Wanted Subjects and Warrants

Total Reported	5273
Confirmed Subject Found	3894
Unconfirmed/Unfound	1379



Adapted from Brooke Powell (Florida Highway Patrol Business Analyst Supervisor), in discussion with the author, October 8, 2015.

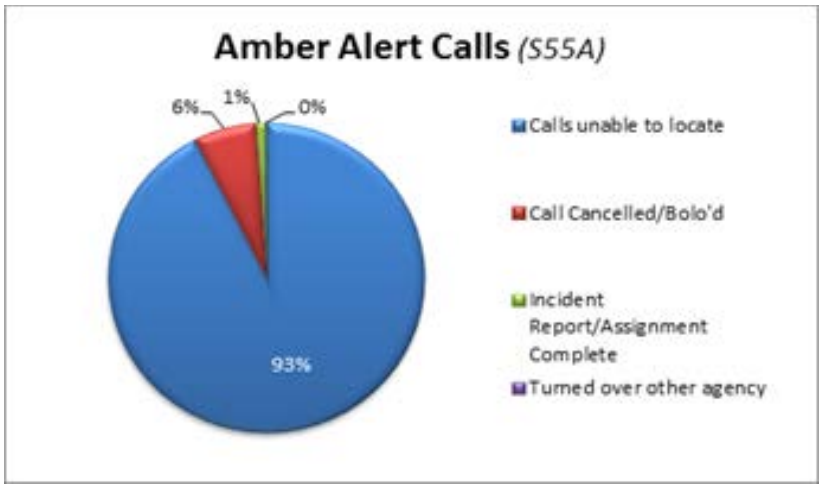
Table 2. Silver Alert Calls

Total Calls Dispatched	9283
Turned over Other Agency	8
Calls Cancelled	603
Located	114
Unable to Locate	8558

Adapted from Brooke Powell (Florida Highway Patrol Business Analyst Supervisor), in discussion with the author, October 8, 2015.

Table 3. Amber Alert Calls

Total Calls Reported	787
Turned over to Other Agency	1
Call Cancelled/Bolo	50
Located	8
Unable to Locate	728



Adapted from Brooke Powell (Florida Highway Patrol Business Analyst Supervisor), in discussion with the author, October 8, 2015.

In analyzing the data, it is apparent that the current methods of locating wanted subjects and Silver and Amber Alert subjects is not overtly affective. In a five-year period, the Florida Highway Patrol dispatched 5,273 calls in an attempt to locate known wanted criminals. They were only successful in apprehending 3,894, which allowed 1,379 subjects to avoid detection and/or further their criminal enterprise. In the same period, the Patrol dispatched 9,283 calls in an attempt to locate Silver Alert subjects. They were only minimally successful, locating 114 subjects and turning over 8 calls to other agencies. The number of unfound Silver Alert subjects, 8,558, although high, may not reflect the entire picture; some of the subjects return home on their own or are located by relatives and other law enforcement agencies prior to getting on the roadway. When looking at the data over the same period concerning Amber Alerts, the Highway Patrol dispatched 787 calls in an attempt to locate these victims. They were only able to locate 8 subjects that were reported missing and/or endangered. The report indicated that 1 case

was turned over to another agency and 50 of the original calls were cancelled. These calls could have been cancelled due to the subject being located during the agency's response.

An analysis of the current systems and processes used to locate and find wanted and missing persons, while widely accepted, allowed over 10,665 subjects to remain undiscovered. No data was maintained by the agency that would support or refute the negative impacts of not locating these missing and wanted subjects. In order to provide supportive data regarding the current systems' effectiveness, it is recommend that agencies create and maintain records that substantiate any positive or negative incidents concerning individuals entered into their system for discovery. Collecting this information will allow further analysis of the positive and negative impacts of not locating the identified target groups and provide evidence supporting research, development and deployment of new technology designed to increase the efficiency of identifying lost, missing and wanted subjects.

THIS PAGE INTENTIONALLY LEFT BLANK

III. LITERATURE REVIEW

This review identifies the current capabilities of facial recognition software (FRS), automatic license plate reader (ALPR) systems and closed-circuit television (CCTV) systems, focusing on how the systems, when combined, could be used to identify suspects that are wanted in connection with a crime, are on the national Terrorism Watchlist, or who have been identified as possible Amber or Silver Alert suspects, while they traverse the U.S. interstate system. It examines the feasibility of combining these systems on a smaller scale, using the Florida turnpike (a limited access highway) as a model.

The Florida Turnpike is designed similarly to other state interstate systems. The proposed system's successful deployment on one interstate system would provide strong evidence that it could be incorporated on others across the nation. In the past few years, law enforcement agencies have been using both FRS and ALPR systems independently as a means of verifying a person's identity or to obtain vehicle information.

Britain has been using a combination of ALPR and CCTV systems for several years in Central London with measurable success. Most notably, these systems were able to identify Robert Thompson and Jon Venables, who were later convicted for the murder of toddler James Bulger, Jr.; identify suspects involved in the 2005 London attacks; identify rioters in the 2011 United Kingdom riots; and obtain footage of Michael Adebolajo and Michael Abebowale, who murdered Lee Rigby in 2013.[92]

In an effort to support the successful merging of these applications (to be used at toll booths on interstate highways) an analysis of the different systems must be conducted. This literature review centers on studies and journal articles that help demonstrate the proposed system's operability, capabilities and limitations regarding privacy issues and civil rights organizations.

[92] "The End of the CCTV Era?," BBC, January 15, 2014, http://www.bbc.com/news/magazine-30793614.

An initial review indicated that the merging of these technologies has not previously been addressed, nor has it been considered as an interstate identification tool. Singularly, all of these technologies work adequately as intended by the manufacturer. Since combining these technologies would be breaking new ground, and because the technologies continue to emerge and evolve, this research resides in the hypothetical-theoretical realm.

The sources used in this literature review have been organized into the following categories:

- Technology
    - Current capability of FRS
    - Current capability of ALPR
    - Current capability of CCTV
- Database capability for FRS, ALPR and CCTV
- Legal review and possible challenges
- Privacy issues and current challenges regarding these technologies
- Records retention concerns
- Policy considerations

Due to corporations limiting the release of specific technical data concerning maximum effectiveness of their systems due to patent laws, this review attempts to conceptualize the feasibility of merging these capabilities; the research is based on the current operational capacity and projected improvement in order to deploy an effective system in addition to forecasting the intended success and or consequences in the formulation of policy.

A. TECHNOLOGY

1. Current Capabilities of Facial Recognition Systems (FRS)

The "U.S. National Institute of Standards and Technology tested an assortment of facial recognition systems in 2010 and established that the top algorithm properly recognized 92% of unidentified persons from a database of 1.6 million criminal records."[93] The findings of these tests were listed in a 2010 report authored by Patrick J. Grother, George W. Quinn and Jonathon Phillips in the NIST Interagency Report titled *Report on the Evaluation of 2D Still-Image Face Recognition Algorithms*.[94] The report is considered accurate by other NIST scholars, including Craig Watson, Brian Cochran and Wayne Salamon, and explains the accuracy of facial recognition technology up to the year of the report.

The Artec Group is recognized as a leader in biometric security and 3D facial recognition technology. The Group reports its systems technical specification and limits on its website, which can be used to compare against others systems for an accurate indication of the facial recognition program's ability to scan moving targets.[95] Even though the pace of a subject walking is considerably slower than a vehicle, it demonstrates the system is capable of scanning moving targets. The technical specification listed by Artec Group for its current system reveals they have the capability of scanning moving targets, which is paramount to demonstrating that the technology is adaptable and feasible.

2. Current Capabilities of Automatic License Plate Readers (ALPR)

In 2012, David Roberts and Meghann Casanova, with the IACP, reviewed license plate reader systems and their associated applications implemented by law enforcement

---

[93] Grother, Quinn, and Phillips. *Report on the Evaluation of 2D Still-Image Face Recognition Algorithms*, 106.

[94] Ibid.

[95] "Artec Group 3D Face Recognition Technology is Represented by a Line of Broadway 3D Biometric Devices," Artec Group, accessed November 22, 2015, http://www.artecid.com/.

agencies within the United States.[96] The IACP was originally developed to assist in apprehending criminals who fled from one jurisdiction to another. Its membership includes police chiefs from around the globe. Over time, the IACP has morphed into the professional voice of law enforcement globally, taking on challenges that address current law enforcement issues by means of providing advocacy, and developing programs and research. The report by Roberts and Casanova assesses ALPR implementation among law enforcement and identifies emerging implementation practices, technical capabilities, current laws, practices and policies in an attempt to provide operational and policy guidance. Their 2012 report provides detailed evidence of the need for both facial recognition and ALPR technologies, and is representative of a small but very valuable literature pool on the end uses of the combined technologies.[97] Further, the report explains the interoperability between ALPR scans and crime system databases used to identify the driver/vehicle owner, vehicle information and wanted or watch list subjects; and outlines policy recommendations pertaining to records retention, deletion and dissemination. The report is considered credible and accurate by the law enforcement community and contributes established policies and procedures that can be used in the development of a system designed to scan interstate traffic for suspect vehicles tied to crimes.[98]

Paul W. Shuldiner, Salvatore A. D'Agostino and Jeffrey B. Woodson's report, published 1996 in the *Journal of the Transportation Research Board*, outlines how the Department of Transportation has used ALPR systems to successfully identify vehicles and their movements in an attempt to "monitor travel time on key roadways for better traffic management" for several years.[99] This report is backed by scientific data and supports the use of ALPR technology to assist in determining vehicle location, based on time and distance, while traveling on interstate systems.

---

[96] "Homepage," The International Association of Chiefs of Police, accessed November 27, 2015 2015, http://www.theiacp.org.

[97] Roberts and Casanova, *Automated License Plate Recognition Systems*, 1.

[98] Ibid.

[99] Paul W. Shuldiner, Salvatore A. D'Agostino, and Jeffrey B. Woodson, "Determining Detailed Origin-Destination and Travel Time Patterns using Video and Machine Vision License Plate Matching," *Transportation Research Record: Journal of the Transportation Research Board* 1551, no. 1 (1996): 8–17.

Continued research and evaluation of research material is ongoing to assess the effectiveness and limitations on ALPRs.

3. Current Capabilities of Closed-Circuit Television (CCTV)

CCTV systems comprise several components, to include a video camera, monitor and a recording device, which are connected to a computer system or other data storage device. Most systems feed the video into a control room that houses the storage solutions and possibly analysis software, depending on the entity deploying the system and the importance of the area under surveillance. Control rooms can be manned or unmanned. Intricate multi-camera systems are designed to allow images to be viewed in chronological order, at the same time, or congruently on numerous monitors at the same time, depending on the system's capabilities. These systems can use a camera that produces a black and white or color picture. New systems utilize digital cameras with infrared to allow visibility in low-light or even no-light conditions. Cameras can be either fixed or varied by remote control, depending on the application, and have the capability to zoom in or out for target acquisition. New technology allows CCTV cameras to be smaller with high definition resolutions, infrared capability allowing night vision and the ability to transmit images over the Internet.[100] Digital video allows for still shots and the capability to zoom in on a target without creating a high level of distortion, as a direct result of the high resolutions produced by the digital camera.

B. DATABASE CAPABILITY FOR FRS, ALPR AND CCTV

The FRS, CCTV and ALPR technologies collect photographic information along with identification information that is acquired though driver's license databases, Department of Correction's booking photographs, the FBI and the National Security Agency, to name a few. Obtaining this information will require policy and regulations to ensure that it is protected from disclosure to unauthorized personnel. FRS will have to be tied to several established photographic databases, as the system relies heavily on

[100] Hernon, "CCTV."

comparison gallery size. The system will not work if a photograph is submitted of a subject that does not have a corresponding photograph in the comparison database.

As a result of the terrorist attacks of September 11, 2001, The United States enacted several new laws, most notably the 2001 Patriot Act and Real ID Act of 2005, in an effort to improve national security. The REAL ID Act (H.R. 1268) was designed based on recommendations of the 9/11 Commission, and is instrumental in improving FRS capability; it was enacted to improve national security efforts and reduce fraud through the standardization of data collection and authentication for state driver's licenses and ID Cards.[101] H.R. 418, "The REAL ID" program, not only forces states to require legal documents—such as birth certificates, passports and other documentation—to ensure applicants are in the United States legally and to verify their identity, but also mandates that states capture a photographed facial image that would allow visual confirmation of the ID to the person holding it.[102] The REAL ID Act also permits interstate sharing of information contained in motor vehicle databases.

To effectively formulate regulations and policies, an analysis of similar database systems currently deployed for similar technology should be completed.

C. INTERSTATE HIGHWAY DESIGN (CURRENT SYSTEMS AND EXISTING INFRASTRUCTURE)

In 2003, the U.S. Department of Transportation release a report revealing roadway mileage and tolls on U.S. interstate highways. This report's data is widely accepted as accurate throughout the U.S., including in the State of Florida. It reports that Florida's turnpike is one of the busiest traveled interstates in Florida, with an average of 1.8 million motorists traversing it daily, and it encompasses over 461 miles of toll-enforced roadway.[103] In addition to the turnpike, Florida has several other toll roads, making it the largest toll-regulated highway in the United States, with a total 657 tolled

[101] Kean, *The 9/11 Commission Report*.

[102] H.R. 418 109th Cong., 1st Session.

[103] "Transportation Statistics: Toll Road Mileage (Most Recent) by State," StateMaster, accessed November 22, 2015, http://www.StateMaster.com/graph/trn_tol_roa_mil-transportation-toll-road-mileage.

miles.[104] This thesis identifies critical information elements to determine if the application of ALPR and FRT will be feasible given the volume of vehicles and the distances traveled.

The Less Stress Roadway Report, published in 2014 by the Florida Turnpike Authority, outlines the systems used on the Florida turnpike for the collection of tolls. It verifies the current use of a toll-by-plate system, which already utilizes photographic license plate readers to run the vehicle's tag through the Division of Motor Vehicles' license plate database and retrieves owner information that can be used by toll officials to seek unremitted payments.[105] Florida's toll system is similar to other state systems, which also require a vehicle to slow down to allow for payment, either manually or electronically. A review of toll speeds coupled with the limitations on FRS and ALPR technology help determine the feasibility of combining these systems.

D. LEGAL REVIEW AND POSSIBLE CHALLENGES

1. Civil Liberties Groups

Several key civil liberty groups, such as the ACLU and the Electronic Frontier Foundation (EFF), have raised concerns that the collection of both photographs and vehicle information from FRS and ALPR systems infringe on a person's right to privacy. The ACLU's 2012 article "You Are Being Tracked" calls privacy rights into question, citing several Amendments to the Bill of Rights. The article provides research that depicts state license plate data retention rates, indicates that information currently collected is used for purposes other than those originally intended, and recommends policies that relate to information sharing and transparency.[106] The literature could provide valuable guidance in writing policies that protect civil liberties without impeding the investigative process.

---

104 "Transportation Statistics," StateMaster.

105 "Florida's Turnpike—The Less Stressway," Florida Turnpike Authority, accessed November 21, 2014, http://www.floridasturnpike.com.

106 "You Are Being Tracked," ACLU.

Currently, no case law or substantiated legal challenges have been noted regarding either FRS or ALPRs within the State of Florida or U.S. Supreme Court. The ACLU and EFF, however, have been distributing public records requests to agencies, including the FBI, in reference to facial recognition programs.[107] In 2009, the IACP conducted a privacy impact study on the use of license plate readers. "The study concluded that LPR systems simply automate the same exact process that has been available to police manually, except ALPR systems simply improve the accessibility of information that is already publicly visible and make it available for analysis and appropriate dissemination."[108] The IACP study further states:

> It should be noted that the enhanced sharing, even among law enforcement personnel, of substantial amounts of information about people not immediately suspected of criminal activity may lead the public to believe that its privacy interests are being ignored….It has been law enforcement's position that the impact of LPR systems on the privacy of individuals is the same as the impact of any ordinary investigation.[109]

The information contained in this study could support the use of ALPR technology against claims by civil liberty groups.

In 2013, Staff Attorney for the ACLU Peter Bibring wrote an article titled "Automated License Plate Readers Threaten our Privacy." In this article, Bibring outlines how some states have limited or outright banned the use of ALPRs due to privacy concerns. The article even references an IACP report, "recognizing that recording driving habit…could raise First Amendment concerns because cameras could record vehicles parked at addiction-counseling meetings, doctors' offices, health clinics or even staging areas for political protest."[110] This article could provide background information on possible legal challenges or attacks that will arise as these systems move forward.

---

[107] Chris Calabrese, "The Biggest New Spying Program You've Probably Never Heard of," ACLU, accessed November, 27, 2015, https://www.aclu.org/blog/biggest-new-spying-program-youve-probably-never-heard?redirect=blog/national-security-technology-and-liberty/biggest-new-spying-program-youve-probably-never-heard.

[108] IACP, *Privacy Impact Assessment Report*.

[109] Ibid.

[110] Peter Bibring and Jennifer Lynch, "Automated License Plate Readers Threaten our Privacy," *Huffington Post*, May 15, 2013, http://www.huffingtonpost.com/peter-bibring/automated-license-plate-readers_b_3231768.html.

Currently, no laws exist in the United States that prohibit the use of facial recognition. However, "based on several provisions in the Bill of Rights, the Supreme Court in Whalen v. Roe held that the right to privacy is one of the most fundamental constitutional rights."[111] This Supreme Court ruling is widely used as a test to determine the constitutionality of methods used in relation to privacy.[112]

There is also no current data to indicate active legal challenges specifically regarding FRS or ALPR systems; however, the ACLU has distributed Freedom of Information Act (FIOA) requests to several entities as a precursor to challenges.[113] A review of privacy acceptance in the United Kingdom was conducted as a guide to determine the best methodology for successful implementation of these technologies, while minimizing privacy concerns, developing policies and building public trust and support. The United Kingdom was selected for review because its laws are more closely related to the United States' than other countries with similar systems; it has the oldest ALPR system in operation, and it has endured several privacy challenges while maintaining a high level of public support.

To determine retention rates for information collected by FRS and ALPR systems, a review of 2014 Florida State Statute, Chapter 119 and Florida Administrative Code was conducted. These resources are critical and maintain compliance to laws regarding destruction of public records in Florida.[114] A National Conference of State Legislatures report, updated in December 2014, provides a state-by-state summary of statutes related to the use of APLRs or retention of data collected by ALPR systems.[115] These laws and reports, which are considered accurate, pertinent and required, are used in conjunction

---

[111] Liu, "Biometrics and Privacy Protection."

[112] *Whalen v. Roe*, 429 U.S. 589, 97 S. Ct. 869, 51 L. Ed. 2d 64 (1977).

[113] "Automatic License Plate Readers FIOA—Lawsuit Complaint," ACLU, accessed November 27, 2015, https://www.aclu.org/legal-document/automatic-license-plate-readers-foia-lawsuit-complaint.

[114] *Public Officers, Employees, and Records*, Title X, Ch. 119, Florida (2014); State of Florida, *General Records Schedule GS1-Sl for State and Local Government Agencies*, (Tallahassee, FL: Florida Department of State, 2013).

[115] "Automated License Plate Readers," National Conference of State Legislatures.

with further reviews of individual state laws and practices to determine best practices in relation to records retention.

2. Court Cases

As privacy concerns are already abundant in regards to these technologies being used singularly, it is anticipated that legal challenges will emerge from the combination of multiple systems. In the absence of pending litigation into privacy concerns specific to this combined technology, a legal review of several court rulings from cases involving privacy issues was conducted to determine possible negative implications, should they be used in challenges. The leading topic of contention by civil liberties groups was the interpretation of the Fourth Amendment to the Constitution: "The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated."[116] The following court rulings were identified and researched to conduct an analysis of the Fourth Amendment to discern if any of its provisions posed a threat to implementation strategies for this proposed system.

Kyllo vs. United States—The Kyllo case revolved around the use of thermal imaging equipment to detect individuals' heat signatures. The Court ruled that, based on definitions outlined in the Fourth Amendment, the use of thermal imaging constituted a "search." The Court went on to discern that looking into a home with the naked eye from a public space, such as a street corner or sidewalk outside a residence, may not be classified as a search. The Court iterated that it is also not considered a search if the police employ technology to replicate what they could see if they were standing on the sidewalk. "The Court went on to add that if technology 'in general public use' is used to see more than the naked eye (e.g., telescope, binoculars, etc.) then it is not a search. 'General public use' is further defined as that which is generally available to the public."[117]

---

[116] "Amendment IV: Search and Seizure," Constitution Center, accessed December 16, 2015, http://constitutioncenter.org/interactive-constitution/amendments/amendment-iv.

[117] *Kyllo v. United States* (99-8508) 533 U.S. 27 (2001) 190 F.3d 1041, reversed and remanded.

Knotts vs. United States—In Knotts vs. United States, the arguments revolved around the "use of CCTV in public spaces and the police's use of a tracking device to track a car through public streets."[118] The Court ruled that the use of this enhanced technology, deployed in the manner it was used in this case, did not constitute an illegal Fourth Amendment search, as the court determined there was no expectation of privacy. "The Court's ruling brought up the question of 'dragnet surveillance,' which the court in U.S. vs. Knotts said would probably be considered a search."[119] In the Court's final ruling, it insinuates that if enhanced surveillance technology is used for extended periods of time—days, weeks or months—an argument could exist that it constitutes a Fourth Amendment search. This type of argument has not been made or considered by the court thus far.

Katz vs. United States—In Katz, the case surrounded the use of audio surveillance placed in a public phone booth. "The Court ruled that surveillance applies to the person and not the location."[120] It added that even though Katz was in public, the act of going into a phone booth was indicative of a person clearly seeking privacy, therefore the expectation of privacy existed; any capture of audio was considered improperly obtained and inadmissible in court.[121] This ruling could be used to argue that the use of CCTV, which captures audio and video could, constitute a Fourth Amendment Search.

The legal analysis yielded inconclusive evidence to support the claim of invasion of privacy due to unreasonable search and seizure.

E. PROCESSES

In the proposed system, data entry in relation to FRS/ALPR scans will be completed both electronically by the equipment and manually by criminal analysts. The facial recognition process involves the collection of the suspect's photographs by digital

---

[118] Department of Homeland Security, *CCTV: Developing Privacy Best Practices* (Washington, DC: Department of Homeland Security, 2007), http://www.dhs.gov/xlibrary/assets/privacy/privacy_rpt_cctv_2007.pdf.

[119] *United States v. Knotts* 460 U.S. 276 (1983).

[120] Department of Homeland Security, *CCTV: Developing Privacy Best Practices.*

[121] *Katz v. United States*, 389 U.S. 347 (1967).

camera, which is then uploaded into a computer program that scans the photograph for possible matches. Once a possible match is obtained, the information, along with the match, is sent to the Criminal Analysis Section for visual comparison and confirmation by a trained analyst. ALPRs use a camera to obtain a photograph of a vehicle's license plate, and then converts the letters or numbers into OCR format. Once the tag is made readable by the software, the program then runs tag information in the Florida Crime Information Center and the National Crime Information Center (FCIC/NCIC) database to determine if the vehicle is connected with a crime, is stolen or has been reported as abandoned. The FCIC/NCIC system returns the vehicle's owner information, and vehicle year, make, model and color. Both systems are monitored by personnel and once a "hit" comes back indicating that the vehicle or person is wanted or suspected of criminal activity, notification is made to law enforcement officers through a 911 center or police dispatch. Once notified, an officer will track down the vehicle and possible suspect and conduct a cursory stop to verify the information. These processes can be completed utilizing a control center that is staffed by a full-time criminal analyst, who can work in real time to discern if a "hit" is positive or negative, allowing them to notify the appropriate law enforcement agency.

IV. ANALYSIS

In comparing the United Kingdom's and the United States' adoption of CCTV, some notable differences were observed. During its first uses in the United Kingdom, governmental officials' initial public support was high, and a lack of legal obstacles allowed for substantial implementation. In this minimally regulated environment, the systems were predicated on self-regulation following a CCTV code of conduct.[122] The U.K.'s CCTV program relies on the Home Office to ensure compliance with the Data Protection Act and the Protection of Freedoms Act, and it applies to both private and public systems. The code of conduct was initiated to ensure that the citizenry and community had confidence that the camera systems deployed were there to protect and support them, rather than to spy on them. The code sets out guiding principles that should apply to all surveillance systems in public places. The intent of these guiding principles was to develop guidelines for operators and users of CCTV systems to ensure proportionality and transparency surrounding their use of surveillance systems. The code is voluntary for all non-relevant entities (private sector), and mandatory for all relevant entities defined as governmental agencies. Failure to comply with the code does not in itself make a non-relevant owner liable to criminal or civil proceedings; however, the surveillance camera code is admissible in evidence in proceedings. Related laws and penalties are outlined in the Data Protection Act of 1998 and the Regulation of Investigatory Powers Act of 2000.[123]

The United States relies more on court rulings and legal opinions in its governance of CCTV systems. In order for the United States to evolve in the area of CCTV systems, it will require legislative action, private and public funding, policy formulation and regulation. This lack of public support will undoubtedly create obstacles for implementing the suggested system.

---

[122] Mark Cole, "Signage and Surveillance: Interrogating the Textual Context of CCTV in the UK," *Surveillance & Society* 2, no. 2/3 (2002).

[123] Home Office, *Surveillance Camera Code of Practice*.

Similar to the United Kingdom, the United States—protected under the Fourth Amendment—widely conducts surveillance of public areas with CCTV. The United States, however, has failed to integrate both private and public CCTV systems to build a network of cameras that are viewed twenty-four hours day. Both the United Kingdom and the United States have integrated ALPR technology in some of their CCTV systems.

The integration of CCTV technology into law enforcement practices has proven to be a costly one. In *Maximum Surveillance Society: The Rise of CCTV*, Clive Norris and Gary Armstrong note that "the exponential increase in visual surveillance creates a massive and costly problem in the area of information processing, storage and handling."[124] Data protection and security are recognized as concerns by both the United Kingdom and the United States, so development of policy is paramount in the successful deployment of CCTV systems.

A key benefit of CCTV systems is personnel efficiency. "Cameras can 'patrol' multiple areas without putting numerous officers on the beat. CCTV videos can be beneficial not only by leading to prompt identification of a suspect, but by providing evidentiary value in court."[125] Public support could be swayed in favor of CCTV systems in public areas if law enforcement could make a case that the systems would provide unbiased visual evidence of police interactions with citizens. This may be useful, as recent negative media coverage of police actions has ignited feelings of mistrust and hatred toward U.S. police officers.

A. LEGAL CONSIDERATIONS

Governmental agencies have issued responses to privacy advocates indicating that no current legislation or restrictions have been ruled on in court concerning CCTV, suggesting that the use of this technology to conduct public surveillance does not violate a person's right to privacy. To date, there have been no constitutional prohibitions concerning visual surveillance systems in public spaces. Some opponents of CCTV say

---

[124] Clive Norris and Gary Armstrong, *The Maximum Surveillance Society: The Rise of CCTV* (Oxford: Berg Publishers, 1999).

[125] Hernon, "CCTV."

that camera monitors constitute unreasonable searches and infringe on the Fourth Amendment right to privacy, while others generally agree there is no reasonable expectation of privacy while out in public, since actions can already be observed indiscriminately by others.[126] The European Commission on Human Rights ruled that no privacy violation has occurred in relation to images taken of persons in public areas, as long as law enforcement does not make images available to the general public.[127]

The United Kingdom allows for subjects to request a copy of any surveillance video/photograph in which they appear. In order to access the information, the subject must complete and submit a form. Entities utilizing CCTV systems, FRS or ALPRs will need to provide strict security of all data collected to ensure that it is only used for official purposes. Development of policies and procedures outlining record retention lengths, sharing and storage would be an area that could come under attack from civil liberties groups.

[126] Robert D. Bickel, *Legal Issues Related to Silent Video Surveillance* (Washington, DC: The Security Industry Association and The Private Sector Liaison Committee,1999).

[127] Ralph Beddard, "Photographs and the Rights of the Individual," *The Modern Law Review* 58, no. 6 (1995): 771–787.

THIS PAGE INTENTIONALLY LEFT BLANK

V. CONCEPTUAL MODELING—HIGHWAY FRS/ALPR APPREHENSION SYSTEM

Using the Florida turnpike as a model, the intent of this chapter is to demonstrate the feasibility of creating a system combining FRS, ALPR and CCTV technologies to locate, track and apprehend or intercept watch list or wanted list suspects and Amber Alert and Silver Alert subjects. Modeling this system on the Florida turnpike will allow other states and municipalities an opportunity to gauge if the system would work within their jurisdictions based on the roadway commonalities. The turnpike was selected as a test roadway in order to afford law enforcement a best-case scenario; on this roadway, law enforcement can track down and stop a suspicious vehicle or person in an isolated area. The shear distance of the turnpike would allow for scans to detect a vehicle's location, and will allow for the computation of time and distance to determine an appropriate interception location.

In order to devise an effective interstate highway/roadway system that can capture both photographs of subjects and license plate information, determining the optimum equipment location is paramount. Current technology can scan automobile license plates on vehicles traveling up to and over 100 miles per hour, which is far better than CCTV's ability to scan a subject's face for use in facial recognition programs. The United Kingdom's uses of CCTV in London Central were successful in part due to the calculated choke points made by officials that limited access points into the city, coupled with several speed bumps placed on the roadway to slow the vehicles down, giving them a good look at the vehicle's tag and the owner.

The Florida turnpike is considered a limited access toll highway; it is controlled by the Florida Department of Transportation and security is provided by the Florida Highway Patrol for all law enforcement responses. The Lake Worth Service Plaza houses the Florida Highway Patrol Communication Center, which monitors live video feeds, intakes calls for service and dispatches law enforcement support. The proposed system will be coordinated and overseen by the Florida Highway Patrol, as it has statewide jurisdiction.

The main roadway extends from Homestead North to Wildwood, located in Sumter County, for a total of 483 miles. The turnpike also includes other sections of toll-enforced highways, to include the Seminole Expressway, Beachline Expressway, Polk Parkway, Veterans Expressway, Suncoast Parkway, the Sawgrass Expressway and the Daniel Webster Beltway and I-4 connector. The main turnpike comprises several on and off ramps along with 63 toll locations, which provide natural choke points. These natural choke points will allow vehicle speeds to decrease significantly, providing the best opportunity to gather useful information from FRS and ALPR equipment. There are eight service plazas located along the main portion of the turnpike. These plazas offer another significant opportunity to gather quality samples for use in FRS and ALPR scans, as vehicles must slow down to enter the plazas. Another useful feature incorporated into the turnpike enterprise is the use of smart message boards. These boards allow the Department of Transportation, in concert with law enforcement, to post information about missing persons and Amber and Silver Alerts to include vehicle make, model and license plate number to allow the motorist to aid in the detection of these subjects or vehicles.

The following section examines some technical consideration used in formulation of this model.

A. TECHNICAL CONSIDERATIONS

"In 2010, NIST tested various facial recognition systems and found that the best algorithms correctly recognized 92 percent of unknown individuals from a database of 1.6 million criminal records."[128] This accuracy was a vast improvement from previous systems and, based on past performance, it is recognized that the technology is still evolving daily. Unfortunately, facial recognition and CCTV systems require a high-quality photograph to ensure accuracy. In modeling this system, care was undertaken to in order to maximize the opportunity for acquisition of useable photographs.

[128] Grother, Quinn, and Phillips, *Report on the Evaluation of 2D Still-Image Face Recognition Algorithms*.

ALPRs are currently capable of scanning and recording plates at the rate of approximately 1 second for vehicles traveling at speeds up to 100 miles per hour.[129] The new ALPR systems utilize infrared cameras which allow significant photographic clarity during night time or daylight hours. The data collected can either be processed immediately (real-time), or it can be transmitted to a control center where it can be processed immediately or stored and analyzed at a later time.

Both FRS and ALPR systems will require a power source and an Internet connection to be operational. This power can be external or internal, with solar power being an option. Internet connectivity must be obtained through hardwire or achieved through wireless connection. This will allow the components to be connected to the control center, with is necessary for operation.

B. CONCEPT

The following elements will be needed to implement a system that combines FRS, ALPR and CCTV on the Florida turnpike to effectively monitor, scan and identify possible watchlist and FBI suspects, state-wanted suspects, and Amber and Silver Alert victims.

1. Control Center/Room

All operations will be facilitated by the control room—a single room designed with multiple monitors, video feeds, computers, telephone systems, database access, and Internet and intranet access. The control center can be attached to the Highway Patrol's Regional Communications Center, or it can be located in an existing building if suitable to mitigate cost. The control center will be operational 24 hours a day, 7 days a week, 365 days a year and will require the staffing and recurring costs projected in Tables 4 and 5.

[129] Manuel D. Rossetti and Jeff Baker, "Applications and Evaluation of Automated License Plate Reading Systems," University of Arkansas, 2001, http://cavern.uark.edu/~rossetti/_Media/its2000paperr2.pdf.

Table 4. Control Center Projected Staff Requirements

Staff Requirement	Number
Staff analysts (entry-level)	18
Analyst supervisors	3
Shift coverage	3 shifts per day
Minimum staffing per shift	3 members
Days worked for staff members	5 days per week

Table 5. Control Center Projected Recurring Annual Costs

Position	Factor	Cost
Staff analysts	Salary per employee (no shift differential figured)	$29,640
	Annual payroll	$533,520
	Annual benefits	$253,422
	Total personnel cost	**$786,942**
Supervisors	Salary per employee (no shift differential figured)	$34,086
	Annual payroll	$102,258
	Annual benefits	$48,573
	Total personnel cost	**$150,831**
Total combined personnel cost		**$937,773**

Projected salaries based on data from www.myflorida.com and http://dmssalaries.herokuapp.com/salaries.

2. CCTV, ALPR Camera Placement

Placement of CCTV systems to capture useable facial photographs for FRS and ALPR cameras to capture vehicle information is critical to the success of this model. Prior to the placement of any capture equipment, it is recommend that tests are conducted to determine the best locations for placement by evaluating daylight, low-light and nighttime conditions. These systems will require a power source, which could be external or internal, utilizing solar power, an Internet connection or wireless capabilities to allow the captures to be sent to the control center. Recommended placement would be at toll plazas and service plazas initially, as they provide basic infrastructure, including lighting, electrical supply and wired Internet capability. These locations also create natural choke points where vehicles slow down to 25 miles per hour or less. Should additional cameras be need, it is recommended that they be placed on on-ramps to gain an initial capture of a vehicle or suspect as they enter the highway system.

3. Database

Currently, the Florida Highway Patrol uses information from FCIC/NCIC databases and DAVID for running vehicle license plates and driver's licenses within the state of Florida. Since July 1, 2010, the DHSMV in the state of Florida has been compiling a driver's license photograph database as a result of the REAL ID Act, which is capable of being filtered through facial recognition software. The database also contains all photographs from state and county corrections facilities though a current MOU. The Highway Patrol should work with the DHSMV to create and maintain its own biometric comparison repository of facial recognition comparison photographs. This repository should tie into the DHSMV driver's license database so that it will continuously update. In an attempt to ensure accuracy, photographs should only be maintained in the database up to 18 months beyond their expiration dates. The separation of the two databases will ensure that both systems are not impacted by each other's use, and allow the Highway Patrol to maintain control and security of their system. This control will minimize the storage space needed to collect and store images within the

system, resulting in reduced cost to the agency and will provide access controls to allow the department to maintain widespread security continuity.

It is recommended that the Florida Highway Patrol reach out to other stakeholders to create information sharing partnerships. These stakeholders should include:

- The 37 Florida county sheriff offices engaged in facial recognition photograph collecting
- Florida Department of Corrections
- Florida Sexual Predators and Offenders database
- The Missing Endangered Persons Information Clearinghouse
- U.S. Department of Justice's Joint Automated Booking System (which collects federal inmate booking images)
- United States Special Operations Command (which houses images of the nation's top most-wanted persons of interest)

For this model to be successfully implemented in other states, it is recommended that the entities overseeing this model work in concert with other state and federal agencies to build an extensive photographic database of terrorist watchlist subjects, FBI most-wanted subjects, wanted subjects and lost and endangered persons. The sharing of this information could be accomplished by issuing MOUs for shared databases. If data cannot be shared or housed in the same database, permissions for access should be granted to an application or portal that would allow the sample photograph to be run against the secure database.

In an effort to safeguard the public from misuse by officials or identity theft, it is advised that the system be built as a closed model and used for official law enforcement purposes only. It is additionally recommended that all photographs of suspects under investigation or arrest be retained until confirmation of the subjects' involvement has been established and the case has been heard in court and closed. Due to current data storage costs, the recommended storage for all data associated with the system that is non-active is 30 days. The system should be designed to dump all captured data that has not been flagged as requiring further investigation or on hold for trial.

4. Scrubbing

Scrubbing is the process of running a digital photograph against a database for comparison. Because of the database size in the proposed system, scrubbing would be taxing and time consuming. In an effort to minimize the time required to process the scan and allow for a subject to be intercepted on the interstate system, it is recommended that the scan be performed in layers based on importance. Priority scanning should be all terrorist watchlist and FBI most-wanted suspects, followed by current missing and endangered persons that are within 48 hours of reporting. The second layer scan should include all endangered and missing persons within the last month and all wanted persons located within the state. The third layer should contain all remaining wanted and missing or endangered persons. This scrub can take place in the background, as the result would be used primarily for follow-up investigation (the length of the scan would most likely not allow for apprehension on the monitored highway, but could provide descriptive information to all other law enforcement agencies).

C. SYSTEM DESIGN

This section describes an aggregate view of what the system could look like, in theory (see Figure 3 for a visual representation). Cameras for capturing facial images and vehicle license plates would be installed at various points, to include toll plazas, service plazas and on-ramps. Signage would be posted to notify subjects that they are being photographed in an attempt to address civil liberty groups' concerns over privacy. The signage would be strategically placed so as to draw the attention of the suspected target toward the camera to allow for optimum capture. The camera systems will transmit the digital images to the control center via Internet or cellular signal, at which time the facial image will be scanned against a controlled database for comparison and the license plate number will be run against the motor vehicle database to determine if it is wanted in connection with a crime, and to provide vehicle registration and identification information that could be used later to locate a suspect.

If the scrub results in a possible match, it will be incumbent on the crime analyst to visually compare the photographs and obtain confirmation with the entity reporting the

status. Once a confirmation is obtained, an officer will be dispatched to intercept the vehicle using its make, model, color and last location as a reference. In cases involving a missing or endangered subject, information can be transmitted to the dynamic message boards, seeking citizens' assistance in locating the vehicle and subject. In most instances, it is advisable to attempt the stop of the subject outside a densely populated area, in which the officer maintains in control of the environment.

Figure 3. Facial Recognition/ALPR System on Interstate System

Images courtesy of INEX/ZAMIR, Florida Center for Investigative Reporting, Penn State, Amazon.com, CCTVFirst, Roberts Space Industries, and *Ocola Post*.

An estimate of the startup cost is not obtainable at this time; it is unknown if available infrastructure is in place to house a crime analysis team or equipment without conducting a feasibility study. It is also unknown if infrastructure is available at equipment installation points to include Internet accessibility, electricity and lighting.

Projected annual salary for staffing of one control center is $937,773, which includes benefits; this cost will be re-occurring (refer to Table 5 on page 54).

The turnpike is operated by the Florida Department of Transportation, which funds all projects, roadway improvements, equipment upgrades and the salaries of state troopers assigned to patrol the turnpike for enforcement activities. It is recommended that federal grants be reviewed and applied for to offset the initial startup cost of this system.

D. BENEFITS

The proposed system would build another layer of protection into our homeland security component. If the system is even moderately successful in apprehending a terrorist suspect or wanted subject, or locates even one lost, endangered or missing subject, it is priceless. According to an Environmental Protection Agency estimate, the United States has one of the highest dollar values of life in the world: $9.1 million.[130] Based on the average value of a single life, the implementation cost and reoccurring operational cost for the proposed system would be minimal in comparison.

[130] Stephanie Chiao, "The Dollar Value of Life," *Metric*, April 20, 2015.

THIS PAGE INTENTIONALLY LEFT BLANK

VI. RECOMMENDATIONS

Since FRS, ALPR and CCTV technology has evolved immensely since its inception, the United States should continue to examine the uses of these technologies by implementing two work groups to study similar systems in the United Kingdom. One work group should study the feasibly, accuracy, effectiveness and possible unintended consequences resulting from the use the systems, while the other should focus on policy, regulation, legal considerations and developing legislation pertaining to the implementation and use of these systems in the United States.

The United States should attempt to mirror the United Kingdom's use of CCTV systems, hoping for similar public acceptance when implementing interstate identification systems. States will have to forge partnerships with other local, county, state and federal law enforcement entities t to increase the net of interstate identification systems, while sharing some of the financial responsibility. The United Kingdom's CTTV program has played an important role in counter-terrorism in general. It is recommended that a study be conducted surrounding the best practices in relation to policy development, procedures and regulations.

The successful implementation of an interstate identification system utilizing FRS, ALPRs and CCTV will require significant buy-in by the American public. This interstate identification system should be sold to the public as another layer in crime prevention and reduction, followed by its homeland security benefits. In an attempt to gain some public support, it is recommended that the U.S. model be as transparent as possible. Businesses and areas under government surveillance should display signage indicating that participants who are in these areas are under surveillance. The goal in the United States should be to develop a surveillance system that deploys a nonintrusive layer of protection to its citizenry.

Law enforcement agencies can leverage these interstate identification systems as a means for deterring crime, even though studies are mostly inconclusive on similar systems effectiveness. In order to gain the public's trust, agencies deploying interstate

identification systems should do so through a joint partnership with the county or city council, mayor, local representatives, community watch groups and local businesses. The use and deployment should be as transparent as possible to gain public trust.

In an effort to ensure that these interstate identification systems are not abused, they should have guidelines and policies that regulate their use, specifically: deployment locations, scope of information collected, records retention lengths, data sharing and data security. Governmental agencies should be required to maintain transparency in their use of the systems.

Legislation should be passed to create a governing body responsible for regulating and ensuring that all government and private entities using interstate identification systems comply with specific rules and regulations both individually and as a unit. Taking a page from the United Kingdom, all identification systems should be assigned a number and registered. This will allow regulators to identify the system and conduct spot checks to ensure compliance with all regulations.

In an attempt to mitigate concerns made by civil liberty groups that suggest videoing persons entering certain establishments (such as churches, polling places, synagogues, abortion clinics, and adult entertainment businesses) violates First Amendment rights, interstate identification systems should only be used to detect and deter criminal or terrorist activities in areas recognized at hot spots or potential targets (critical infrastructures). Camera placement should be regulated to ensure placement does not pose a threat to civil liberties, while still providing a level of security, maintaining its functionality and its ability to deter possible terrorist activity. Information collected from the systems should only be used as evidence in criminal investigations, terrorist investigations or internal disciplinary procedures.

Developing a system that combines FRS, ALPRs and CCTV to identify watchlist suspects, wanted criminals, missing subjects, and Amber and Silver Alert victims makes sense. All three of these systems will be tied into a larger network of systems to achieve success. This could be considered a system of systems—a system with interconnected

sets of elements organized to achieve a combined goal.[131] It is a practical attempt at stopping a terrorist attack prior to its implementation stage.

Two distinct challenges will arise in the development of such a tool. The first will be the process of developing policies for how the system will function, how it will work harmoniously with other systems, how the records created by the system will be reviewed and retained and how operators and users will be trained. The policy will have to have specific values placed on public acceptance and privacy issues in order to be successful. The elephant in the room concerning this project will be funding. Decision makers should keep in mind that if the system is able to identify and apprehend a single dangerous subject, it should be deemed a success. If the system finds a wanted suspect or missing subject, it can also seek funding tied to a homeland security grant.

The largest struggle or challenge for this type of system will be competing for funds against other similar programs designed to stop terrorism. In formulating a strategy, an expansive look at CCTV systems in London Central will be conducted to analyze its effectiveness. The short-term strategy is implementing this system in a smaller, more controlled environment, such as the Florida turnpike system. The turnpike has a few natural choke points similar to London Central that would eliminate the need for new infrastructure.

Legislature and new laws will need to outline how the system will be utilized, as well as requirements for privacy, record sharing and records retention. Following legislative support, the agency will need to garner support from the public and privacy groups. The chart in Table 6 identifies the different groups that are necessary for successful implementation and deployment of this system.

[131] Donella H. Meadows, and Diana Wright, *Thinking in Systems: A Primer* (White River Junction, VT: Chelsea Green Publishing, 2008).

Table 6. Stakeholders for System Implementation

Group	Nominal Selectorate Interchangeable	Real Selectorate Influentials	Winning Coalition Essential
Facial Recognition	• General public • Facial recognition technology • Manufactures • Suppliers • Public/private sector	• Florida Highway Patrol • Policymakers • Stakeholders • Legislatures/lobbyists • Governance • Grant Writers	• Manufacturers • Suppliers • Installers • Stakeholders • Public • Contract awardees • Public sector • Media • Privacy advocates
Automatic License Plate Readers	• General public • ALPR manufacturers • Suppliers • Public/private sector	• Florida Highway Patrol • Policymakers • Stakeholders • Legislatures/lobbyists • Governance • Grant writers	• Manufactures • Suppliers • Installers • Stakeholders • Public • Contract awardees • Public sector • Media • Privacy advocates
CCTV	• General public • CCTV manufacturers • Suppliers • Public/private sector	• Florida Highway Patrol • Policymakers • Stakeholders • Legislatures/lobbyists • Governance • Grant writers	• Manufacturers • Suppliers • Installers • Stakeholders • Public • Contract awardees • Public sector • Media • Privacy advocates
Other Associated Technology/ Equipment	• General public • Equipment manufacturers • Suppliers • Public/private sector	• Florida Highway Patrol • Policymakers • Stakeholders • Legislatures/lobbyists • Governance • Grant writers • U.S. DOT • FLA DOT	• Manufacturers • Suppliers • Installers • Stakeholders • Public • Contract awardees • Public sector • Media • Privacy advocates

In today's media-frenzied world, several entities and sub-entities would need to work together to formulate a strategy and policy for success; in Table 6, these groups are called selectorates. In building a successful roadmap for implementation, the groups have been broken down by technology. The first group—nominal or interchangeable—includes all entities or persons that will have a say in the development and implementation of the systems they support.[132] The second group—influentials—represents those who will be responsible for the formulations of strategies for implementation, policy creation, deployment, gaining public support, lobbying for laws that will support the system or provide oversight in relations to records retention and privacy advocacy. This group is critical to any successful deployment and usage of the system. The last group is the winning coalition.[133] It includes several components from the previous influential grouping. This group will either support or protest the implementation of the components needed to provide a working system. It is at this stage in the process that the determination of system success or failure will occur.

Knowing how these groups work in concert will allow for strategic planning and subsequently successful implementation. Once the concept is formulated, several factors will influence how it advances from invention to deployment. Research and development will take place, along with a process of vetting equipment manufacturers. This vetting process will be based on the capabilities of the systems offered by different manufacturers' costs, and their ability to merge or coexist with the other systems required. In state government, a bid process would be utilized, provided the company is not a single-source provider. Once the bids are completed, budget considerations will occur. The finance department will determine if there are funds available or if a grant would have to be proposed for funding. They will also determine if source funding is allowed by finance laws through the legislature. The finance department will look at the project and project the cost and value, and will have to analyze what reoccurring cost would be necessary to maintain the system. While budget considerations are underway,

[132] Bruce Bueno De Mesquita and Alastair Smith, *The Dictator's Handbook: Why Bad Behavior Is Almost Always Good Politics* (New York: Public Affairs, 2011).

[133] De Mesquite and Smith, *The Dictator's Handbook*, 28.

department leaders, stakeholders, legal parties and lobbyists will determine the constitutionality of the system, and will consider current privacy laws or social media pressure.

Unfortunately, lobbyist and legislative bodies can be influenced by advocacy groups. It is imperative that the department work in concert with them, the media and privacy groups in an attempt to garner support and buy-in prior to the implementation phase. Open dialog, transparency and input from various groups will undoubtedly help create cohesion, making public support easier to obtain and implementation and deployment successful. Manufacturers often enlist lobbyists to assist them in brokering deals with lawmakers when the repeal or creation of a law is advantageous to their business. The department should consider this partnership to help create laws that could aid in the deployment of this program.

Legislative and public acceptance is critical to this program's success, especially knowing that they are influenced by big business and constituents equally. Money influences manufacturers, as their viability relies on sales. Lobbyists are paid by entities to influence lawmakers to get favorable laws to allow their technology to advance. Lawmakers, however, are often controlled by the voting base within their districts and they are responsive or unresponsive based on what is in their best interest at the time. Media and privacy groups get their power from controversy; the more controversial, the more sales they acquire.

For successful deployment, leaders, policymakers and decision makers need to formulate a strategy that involves groups and subgroups that support the mission or have a common interest in the successful incorporation of specific components. These groups can have different specific interests for the success or implementation— manufacturers are in it for profit, lobbyists for public support, law enforcement for security and safety, media for profit or readership, and advocacy groups/privacy groups for followership or media attention. In any development of policy, it is imperative to leverage your relationships, foster new relationships, garner outside support and build a coalition of entities that will have a similar interest in obtaining your goal, even though their end result may differ from yours.

VII. CONCLUSION

Historically, law enforcement has come under increased scrutiny for perceived violations of personal privacy. With technology advances, civil liberties groups and/or anti-government groups will likely find fault with these new technologies and processes. Due to the attacks of September 11, 2001, public support is still leaning in favor of law enforcement, thus allowing a broader interpretation of laws on privacy issues surrounding the need to protect our nation from terrorist attacks. The public and the courts have been increasingly accepting and tolerant of methods used by police in attempt to keep the nation safe. For example, in the 2013 Supreme Court case Maryland v. King, the Court ruled that the "DNA identification of arrestees is a reasonable search that can be considered part of a routine booking procedure," akin to fingerprinting and photographing.[134] This case allows for the collection and preservation of DNA samples that could be cataloged and used later to confirm or refute a subject's involvement in a crime upon arrest and not conviction, which shocked civil liberties groups. One could argue based on this ruling that a photograph of a non-arrested subject would be acceptable for use in a facial recognition program without a violation of privacy rights. The further we are removed from September 11, however,, the raw emotions associated with the attacks will wane, resulting in the de-escalation of public support for law enforcement and government protections. The eroding of this public trust and support will undoubtedly make technology such as FRS, ALPRs and CCTV harder to present to the masses.

Facial recognition is an advancing technology that has the potential to be a very effective tool in identifying known suspected criminals, thwarting terrorism, and reducing fraud and identity theft. In general, these systems are less intrusive, allowing them to be deployed remotely, without the individuals knowing that their images were captured.[135] To be effective, agencies will have to use the technology appropriately and safe guard

---

[134] *Maryland v. King, S.C,* 133, No. 12–207 (2013): 1958.

[135] "State Photo-ID Databases Become Troves for Police," *Washington Post*," June 16, 2013, http://www.washingtonpost.com/business/technology/state-photo-id-databases-become-troves-for-police/2013/06/16/6f014bd4-ced5-11e2-8845-d970ccb04497_story.html.

vital information transparently in order to maintain the trust and confidence of the American people. In protection of these systems, agencies must maintain strict adherence to informational safeguard practices and conduct routine audits designed to minimize abuses or unlawful practices. Time and technological advances will ultimately decide the value of FRS and its effectiveness as a law enforcement tool. If one life lost is considered too much, one could surmise that law enforcement agencies have the inherent responsibility to actively seek out and deploy new tools and technologies in their effort to provide a safe environment.

It is believed that this thesis will serve as a catalyst for the formation of a new security system designed to locate, identify and apprehend know terrorist watchlist suspects and other wanted persons who are traversing U.S. interstate systems. The goal is to provide another layer of protection and create a deterrent for terrorist suspects. As previously discussed, it is believed that this thesis will open the eyes of the public, law enforcement, judicial circuits and civil liberty groups to this technology's possible impact on homeland security. It is anticipated that the reader will have an understanding of the systems, to include their general capabilities.

In looking at the policy side of the thesis, recommendations for changes have been provided to support or defend legal challenges, allowing department heads and administrators to make informed policy and operational practices decisions.

APPENDIX.

Sample of FBI MOU for the Interstate Photo System Facial Recognition Pilot. Source: Jennifer Lynch, "FBI Plans to Have 52 Million Photos in its NGI Face Recognition Database by Next Year," Electronic Frontier Foundation, accessed August 28, 2014. https://www.eff.org/deeplinks/2014/04/fbi-plans-have-52-million-photos-its-ngi-face-recognition-database-next-year.

MEMORANDUM OF UNDERSTANDING
BETWEEN
THE FEDERAL BUREAU OF INVESTIGATION
AND
(STATE/ AGENCY)
FOR THE
INTERSTATE PHOTO SYSTEM FACIAL RECOGNITION PILOT

GENERAL PROVISIONS

1. PURPOSE: This Memorandum of Understanding (MOU) between the Federal Bureau of Investigation (FBI), Criminal Justice Information Services (CJIS) Division, and the (STATE/AGENCY), hereinafter referred to as the 11Parties, 11 is for the limited purpose of testing and piloting the FBI's Interstate Photo System Facial Recognition Pilot (IPSFRP). This MOU memorializes the Parties' understandings regarding the transmittal, receipt; storage, use, and dissemination of information relating to this piloting initiative.

2. BACKGROUND: The FBI maintains millions of digital representations of fingerprint images, features from digital fingerprint images, and associated criminal history record information in the Integrated Automated Fingerprint Identification System (IAFIS). The IAFIS provides automated fingerprint search capabilities, latent print search capabilities, electronic image storage and electronic exchange of fingerprints, criminal history and associated photos to support law enforcement and authorized civil organizations. Collectively, "this data comprises the biometric content, format, and units of measurement for the electronic exchange of information that may be used for positive fingerprint identifications. Given the advances in biometric identification technology, including hardware, software, and digital imaging, it is essential that existing search capabilities be enhanced to meet authorized customer needs. The CJIS Division's Next Generation Identification (NGI) System expects to reduce terrorist and other criminal activities by implementing multiple search capabilities that will improve, expand, or create new biometric identification tools and investigative services for the FBI's user community.

The IPSFRP satisfies a subset of the NGI Interstate Photo System (IPS) requirements, and a prototype system was delivered to assist in the development of the IPS facial

recognition system. Upon full implementation, IPS enhancements will: 1) expand storage capacity, thereby allowing a more robust photo repository; 2) permit photo submissions independent of arrests; 3) permit bulk submission of photos being maintained at state and federal repositories; 4) accommodate the submission and searching of non-facial photos (e.g., Scars, Marks and Tattoos [SMTs]); 5) permit IPS photo retrieval via the National Crime Information Center (NCIC); and 6) provide facial recognition search capabilities.

It is important to note that although facial recognition technology has been under development since the 1960s, universal algorithmic approaches for facial recognition do not exist. Approaches originally tailored to low resolution, two-dimensional images have been improved to account for greater levels of resolution and three-dimensional data. The U.S. Government has performed multiple evaluations of facial recognition technology and preliminary results demonstrate that accuracy has greatly improved. Accordingly, these enhancements support the FBI's decision to enhance 'its photo processing capabilities in the early stages of NGI system development, to include facial recognition technology.

To address and enhance photo processing capabilities, the FBI is initiating the IPSFRP as a collaborative effort to identify user needs, provide proof of concept, establish thresholds for lights out searches at the national level and develop a useful investigative tool for the law enforcement community.

Agencies participating in this pilot program have implemented a facial recognition system for investigative, identity authentication and/or tracking purposes. In support of this initiative, the (STATE/AGENCY) will submit images to a state/regional photo repository and the repository will provide search results to the submitting law enforcement agency. The (STATE/AGENCY) will also request that the photo submission be forwarded to the CJIS Division; via the CJIS Wide Area Network (WAN) or other FBI approved secure web services, for comparison against the FBI's national photo repository. This pilot is designed to provide participating law enforcement agencies an automated facial recognition search of a subset of the FBI's national photo repository until full implementation of the IPS facial recognition search capability in 2014. The IPSFRP will represent a subset of the IPS repository and will be expanded and updated periodically throughout the pilot. The subset repository will not represent a real time reflection of the IPS or Interstate Identification Index (III) photo repository.

Technical specifications for the IPSFRP are derived from the CJIS Electronic Biometric Transmission Specification (EBTS) and the American National Standards Institute (ANSI) American National Standard for Information Systems- Data Format for the Interchange of Fingerprint, Facial, & other Biometric Information.

During the IPSFRP piloting phase, relevant transactions will be analyzed by the Parties and their authorized contractors to assess system performance. In addition, the NGI IPS system design will be recording lessons learn and user input.

System availability will be limited during this initiative. Accordingly, the CJIS Division will provide advanced notice of sporadic system availability, backup recovery limitations, and failover shortfalls during the prototype phase. In addition, the CJIS Division may limit the number of transactions that will be accepted during the pilot phase.

3. AUTHORITY: The FBI enters into this MOU under the statutory authority provided by Title 28, United States Code, § 534. The (STATE/AGENCY) enters into this MOU pursuant to
(STATE STATUTE/CODE)

4. SCOPE: This MOU applies to facial photo images provided by the (STATE/AGENCY) and he FBI's responses.

A. The FBI will:
1. Accept one frontal facial photo submission per IPSFRP search request;

2. Search each frontal facial image against the IPSFRP national repository;

3. Provide a candidate list per each applicable IPSFRP search request. The candidate list will contain the agency's requested number (minimum of2) of candidates or a default number of 20 candidates if not specified by the agency, as well as a caveat message;

4. Provide a valid FBI identifier for each candidate;

5. Maintain a log of all transactions and disseminations;

6. Designate a point of contact (POC) for issues and concerns related to this initiative;

7. Conduct post processing on submitted transactions to determine system performance and miss analysis and provide results to the submitting agency; and

B. The (STATE/AGENCY) will:

1. Submit no more than one frontal facial photo (EBTS - ANSI compliant) per IPSFRP search request via the CJIS WAN or other FBI approved secure web services;

2. Request a specified number (minimum of 2, default of 20, maximum of 50) of returned candidates;

3. Conduct a search of the III to ensure information derived from the IPSFRP candidate lists are up to date;
4. Disseminate FBI responses to authorized criminal justice recipients as an investigative lead;

A. Provide the CJIS Division with post processing results, such as:

1. Agency identified a subject from the candidate list and what rank.
2. Search resulted in an investigative lead.
3. Search was of no value

B. Designate a POC for issues and concerns related to this initiative.

5. DISCLOSURE AND USE OF INFORMATION: The IPSFRP pilot search will be limited to authorized criminal justice agencies for criminal justice purposes. The IPSFRP, and the photo search thereof, is considered to be a part of the IAFIS, therefore all CJIS rules regarding access to IAFIS and dissemination/use of FBI provided information will apply. The Parties acknowledge that information involved in this initiative may identify United States persons, whose information is protected by the Privacy Act of 1974, Executive Order 12333, any successor executive order, or other federal authority. Accordingly, all such information will be treated as "law enforcement sensitive" and protected from unauthorized disclosure. Each Party will immediately report to the other Party any instance in which data received from the other Party is used, disclosed, or accessed in an unauthorized manner (including any data losses or breaches).

Information derived from the FBI IPSFRP search requests and resulting responses are to be used only as investigative leads. Though there are expected to be similarities between submitted images and candidate lists, results shall not be considered to be positive identifications nor considered to have active warrants. Although the emerging technology of facial recognition has made great strides over the years, facial recognition initiatives are not deemed to provide positive identifications and the Parties are prohibited from relying solely on IPSFRP search responses as the sole impetus for law enforcement action. Other indicators and factors must be considered by the submitting agency prior to making an identification.

6. FUNDING: There are no reimbursable expenses associated with this level of support. Each
Party will fund its own activities unless otherwise agreed to in writing. Expenditures will be subject to budgetary processes and availability of funds and resources pursuant to applicable laws, regulations and policies. The Parties expressly acknowledge that this MOU in no way implies that Congress or the State of (STATE/ AGENCY) will appropriate funds for such expenditures.

7. SETTLEMENT OF DISPUTES: Disagreements between the Parties arising under or relating to this MOU will be resolved only by consultation between the Parties and will not be referred to any other person or entity for settlement.

8. SECURITY: It is the intent of the Parties that the' transfer of information described under this
MOU will be conducted at the unclassified level. Classified information will neither be provided nor generated under this MOU.

9. AMENDMENT and TERMINATION:

A. All activities under this MOU will be carried out in accordance to the above described provisions.

B. This MOU may be amended or terminated at any time by the mutual written consent of the Parties' authorized representatives.

C. Either Party may terminate this MOU upon thirty (30) days written ·notification to the other Party. Such notice will be the subject of immediate consultation by the Parties to decide upon the appropriate course of action. In the event of such termination, the following rules apply:

1. The Parties will continue participation, financial or otherwise, up to the effective date of termination.

2. Each Party will pay the costs it incurs as a result of termination.

3. All information, copies thereof, and rights therein received under the provisions of this MOU prior to the termination will be maintained in accordance with the receiving Party's practices.

10. ENTRY INTO FORCE, AND DURATION: This MOU, which consists often Sections, will enter into effect upon the signature of both Parties, will be reviewed annually, on or prior to the anniversary date, to determine whether amendments are needed, and will remain in effect until terminated or completion of the testing and piloting phase. This MOU is not intended, and should not be construed, to create any right or benefit, substantive or procedural, enforceable at law or otherwise by any third party against the Parties, their parent agencies, the United States or the officers, employees, agents, or other associated personnel thereof.

The preceding ten (1 0) sections represent the understandings reached between the FBI and the (STATE/AGENCY)

FOR THE FEDERAL BUREAU OF INVESTIGATION

_____

David Cuthbertson
Assistant Director
Criminal Justice Information Services Division
Federal Bureau of Investigation

FOR THE (STATE/AGENCY)

_____

John Doe
Attorney General
(STATE/AGENCY)

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF REFERENCES

ACLU. "ACLU Releases Documents on License Plate Scanners from some 300 Police Departments Nationwide." July 17, 2013. https://www.aclu.org/technology-and-liberty/aclu-releases-documents-license-plate-scanners-some-300-police-departments.

———. "Automatic License Plate Readers FIOA—Lawsuit Complaint." Accessed November 27, 2015. https://www.aclu.org/legal-document/automatic-license-plate-readers-foia-lawsuit-complaint.

———. "You Are Being Tracked: How License Plate Readers Are Being Used to Record Americans' Movements." Accessed July 26, 2014. https://www.aclu.org/technology-and-liberty/you-are-being-tracked-how-license-plate-readers-are-being-used-record.

Al Franken Senator for Minnesota. "Sen. Franken Raises Concerns about Facial Recognition App that Lets Strangers Secretly Identify People." February 5, 2014. http://www.franken.senate.gov/?p=press_release&id=2699.

Armitage, Rachel. "To CCTV or Not to CCTV: A Review of Current Research into the Effectiveness of CCTV Systems in Reducing Crime." Nacro. May 2002. https://epic.org/privacy/surveillance/spotlight/0505/nacro02.pdf.

Artec Group. "Artec Group 3D Face Recognition Technology is Represented by a Line of Broadway 3D Biometric Devices." Accessed November 22, 2015.

Ball, Kristie, David Lyon, David Murkami Wood, Clive Norris, and Charles Rabb. *A Report on the Surveillance Society*. United Kingdom: Surveillance Studies Network, 2006. https://www.priv.gc.ca/information/int/2006/surveillance_society_full_report_2006_e.pdf.

BBC. "The End of the CCTV Era?" January 15, 2014. http://www.bbc.com/news/magazine-30793614.

———. "Privacy Fears over FBI Facial Recognition Database." April 15, 2014. http://www.bbc.com/news/technology-27037009

Beddard, Ralph. "Photographs and the Rights of the Individual." *The Modern Law Review* 58, no. 6 (1995): 771–787.

Bibring, Peter and Jennifer Lynch. "Automated License Plate Readers Threaten our Privacy." *Huffington Post*. May 15, 2013. http://www.huffingtonpost.com/peter-bibring/automated-license-plate-readers_b_3231768.html.

Bickel, Robert D. *Legal Issues Related to Silent Video Surveillance*. Washington, DC: The Security Industry Association and The Private Sector Liaison Committee,1999.

Biometric-Solutions. "Biometrics." Accessed November 27, 2015. http://www.biometric-solutions.com/index.php.

Blackburn, Duane M., Mike Bone, and P. Jonathon Phillips. *Facial Recognition Vendor Test 2000: Evaluation Report*. Washington, DC: National Institute of Justice, 2001. http://www.bioconsulting.com/Facial_Recognition/FRVT_2000.pdf.

Calabrese, Chris. "The Biggest New Spying Program You've Probably Never Heard of." ACLU. Accessed November, 27, 2015. https://www.aclu.org/blog/biggest-new-spying-program-youve-probably-never-heard?redirect=blog/national-security-technology-and-liberty/biggest-new-spying-program-youve-probably-never-heard.

Coaffee, Jon "Rings of Steel, Rings of Concrete and Rings of Confidence: Designing out Terrorism in Central London Pre- and Post- September 11th." *International Journal of Urban and Regional Research* 28, no. 1 (2004): 201–211.

Cole, Mark. "Signage and Surveillance: Interrogating the Textual Context of CCTV in the UK." *Surveillance & Society* 2, no. 2/3 (2002).

Constitution Center. "Amendment IV: Search and Seizure." Accessed December 16, 2015. http://constitutioncenter.org/interactive-constitution/amendments/amendment-iv.

Dailey, Kate. "The Rise of CCTV Surveillance in the US." *BCC News Magazine*. April 29, 2013.

Death and Taxes. "FBI Introduces Next Generation Facial Recognition Technology." October 20, 2011. http://www.deathandtaxesmag.com/152857/fbi-introduces-next-generation-facial-recognition-technology/.

De Mesquita, Bruce Bueno and Alastair Smith. *The Dictator's Handbook: Why Bad Behavior Is Almost Always Good Politics*. New York: PublicAffairs, 2011.

Department of Homeland Security. *CCTV Developing Privacy Best Practices* Washington, DC: Department of Homeland Security, 2007. http://www.dhs.gov/xlibrary/assets/privacy/privacy_rpt_cctv_2007.pdf.

Dowden, John. "Facial Recognition: The Most 'Natural' Forensic Technology." *Evidence Technology Magazine* 11, no. 5 (September–October, 2013). http://www.evidencemagazine.com/index.php?option=com_content&task=view&id=1344.

Edwards, P. and N. Tilley. *CCTV–Looking Out for You*. London: Home Office, 1994.

FBI. *Striking a Balance—A Government Approach to Facial Recognition Privacy and Civil Liberties* (U.S. Government Facial Recognition Legal Series Forum 2). Washington, DC: Department of Defense, 2012.

Florida Highway Safety and Motor Vehicles. "DAVID—Law Enforcement's Best Information Tool." *Legal Highway* III, no. 1 (Spring/Summer, 2013): 1.

Florida Turnpike Authority. "Florida's Turnpike—The Less Stressway." Accessed November 21, 2014. http://www.floridasturnpike.com.

Fox 5 Las Vegas. "Power Struggle: Customers vs. NV Energy Smart Meters."February 6, 2015. http://www.fox5vegas.com/story/16689913/a-charged-debate-customers-vs-nv-energy-smart-meters.

Gastañaga, Claire Guthrie. "Protecting Privacy while Keeping Us Safe: Technology and Liberty." ACLU. June 4, 2014/ http://acluva.org/15321/protecting-privacy-while-keeping-us-safe-technology-and-liberty/.

Gill, Martin and Angela Spriggs. *Assessing the Impact of CCTV*. London: Home Office Research, Development and Statistics Directorate, 2005.

Goldstein, A. J., L. D. Harmon, and A. B Lesk. "Identification of Human Faces." In *Proceedings of IEEE* 59, no. 5 (May 1971): 748–760.

Gras, Marianne L."The Legal Regulation of CCTV in Europe." *Surveillance & Society* 2, no. 2/3 (2002).

Grother, Patrick J., George W. Quinn, and P. Jonathon Phillips, *Report on the Evaluation of 2D Still-Image Face Recognition Algorithms* (NIST Interagency Report 7709). Gaithersburg, MD: NIST, 2010.

Hempel, Leon and Eric Topfer. *CCTV in Europe: Final Report* (Working Paper No. 15). Berlin: Technical University Berlin, 2004. http://www.urbaneye.net/results/ue_wp15.pdf.

Hernon, Jolene. "CCTV: Constant Cameras Track Violators." *NIJ Journal*, no. 249 (2003): 16–23.

History of Forensic Psychology. "Face Recognition Software." Accessed December 5, 2015. http://forensicpsych.umwblogs.org/research/criminal-justice/face-recognition-software.

Home Office. *Surveillance Camera Code of Practice*. London: The Stationary Office, 2013. https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/204775/Surveillance_Camera_Code_of_Practice_WEB.pdf.

IACP. “Homepage.” Accessed November 27, 2015 2015. http://www.theiacp.org.

———. *Privacy Impact Assessment Report for the Utilization of License Plate Readers.* Alexandria, VA: International Association of Chiefs of Police, 2009.

Jones Jr., Marshall.”Who Invented the First CCTV System?” Sonitrol. June 30. 3014, http://www.sonitrolky.com/invented-first-cctv-system/.

Kean, Thomas. *The 9/11 Commission Report: Final Report of the National Commission on Terrorist Attacks upon the United States*. Washington, DC: Government Printing Office, 2011.

Klontz, Joshua C. and Anil K. Jain. *A Case Study on Unconstrained Facial Recognition Using the Boston Marathon Bombings Suspects* (Tech. Rep. MSU-CSE-13-4). Lansing, MI: Michigan State University, 2013.

Liu Yue. “Biometrics and Privacy Protection in USA’s Constitution.” *International Journal of Private Law* 4, no. 1/2110 (January, 2011): 54–68.

Lum, Cynthia, Linda Merola, Julie Willis, and Breanne Cave. *License Plate Recognition Technology (LPR):Impact Evaluation and Community Assessment*. Fairfax, VA: George Mason University, 2010.

Lynch, Jennifer. “FBI Plans to Have 52 Million Photos in its NGI Face Recognition Database by Next Year.” Electronic Frontier Foundation. April 14, 2014. https://www.eff.org/deeplinks/2014/04/fbi-plans-have-52-million-photos-its-ngi-face-recognition-database-next-year.

McCahill, Michael and Clive Norris. *CCTV in Britain* (Working Paper No. 3). Berlin: Technical University Berlin, 2002.

———. *CCTV Systems in London: Their Structure and Practices* (Working Paper No. 10). Hull, UK: University of Hull, 2003.

McDermott, Terry. *Perfect Soldiers: The Hijackers: Who They Were, Why They Did It*. New York: Harper Collins, 2005.

Meadows, Donella H. and Diana Wright. *Thinking in Systems: A Primer*. White River Junction, VT: Chelsea Green Publishing, 2008.

MPDC. “MPDC’s Closed Circuit Television (CCTV) System.” Accessed May 27, 2015. http://mpdc.dc.gov/page/mpdcs-closed-circuit-television-cctv-system.

The National Archives. “Data Protection Act 1998.” Accessed December 17, 2015, http://www.legislation.gov.uk/ukpga/1998/29/contents.

National Conference of State Legislatures. "Automated License Plate Readers, State Statutes Regulating Their Use." February 2, 2015. http://www.ncsl.org/research/telecommunications-and-information-technology/state-statutes-regulating-the-use-of-automated-license-plade-readers-alpr-or-alpr-data.aspx.

National Science and Technology Council. "*Face Recognition*." Biometrics.gov. August 7, 2006. http://www.biometrics.gov/Documents/FaceRec.pdf.

Nichols, Laura J. *The Use of CCTV/Video Cameras in Law Enforcement*. Alexandria, VA: International Association of Chiefs of Police, March 2001.

Norris, Clive and Gary Armstrong. *The Maximum Surveillance Society: The Rise of CCTV*. Oxford: Berg Publishers, 1999.

Reese, Shawn. *National Special Security Events* (CRS Report No. RS22754). Washington, DC: Congressional Research Service, 2007.

Reeve, Tom. "How Many Cameras in the UK? Only 1.85 Million, Claims ACPO Lead on CCTV." Security News Desk. March 2011.

Roberts, David J. and Meghann Casanova. *Automated License Plate Recognition (ALPR) Systems: Policy and Operational Guidance for Law Enforcement.* Washington, DC: National Institute of Justice, 2012.

Rossetti, Manuel D. and Jeff Baker. "Applications and Evaluation of Automated License Plate Reading Systems." University of Arkansas. 2001. http://cavern.uark.edu/~rossetti/_Media/its2000paperr2.pdf.

Ruberto, Jacob. "Interagency use of Facial Recognition." Atlanta, GA: Pinellas Sheriff's Office, 2013.

Rucke, Katie. "'Startling' Number of Americans are on Terrorist Watchlist." *Mint Press News*. Accessed July 23, 2014. http://www.mintpressnews.com/startling-number-of-americans-are-on-terrorist-watchlist/194356.

Russell, Brandon. "Why Facebook is Beating the FBI at Facial Recognition." The Verge. July 7, 2014. http://www.theverge.com/2014/7/7/5878069/why-facebook-is-beating-the-fbi-at-facial-recognition.

Schlosberg, Mark and N. Ozer. *Under the Watchful Eye: The Proliferation of Video Surveillance Systems in California*. New York: American Civil Liberties Union, 2007.

Shah, Rajiv and Jeremy Braithwaite. "Spread Too Thin: Analyzing the Effectiveness of the Chicago Camera Network on Crime." *Police Practice and Research* 14, no. 5 (2013): 415–427.

Shockley, B. “Lawsuit Challenges State of Utah Ban on License Plate Readers.” Vigilant Solutions. February 13, 2014. http://vigilantsolutions.com/press/drn_vigilant_utah_lpr_federal_lawsuit.

Shuldiner, Paul W., Salvatore A. D’Agostino, and Jeffrey B. Woodson. “Determining Detailed Origin-Destination and Travel Time Patterns using Video and Machine Vision License Plate Matching.” *Transportation Research Record: Journal of the Transportation Research Board* 1551, no. 1 (1996): 8–17.

Sirovich, Lawrence and Michael Kirby. “Low-Dimensional Procedure for the Characterization of Human Faces.” *Journal of the Optical Society of America* 4, no. 3 (1987): 519–524.

SRMTI. “The History of CCTV in the UK.” Sccessed November 27, 2015. http://www.srmti.com/news/the-history-of-cctv-in-the-uk-10079/.

State of Florida. *General Records Schedule GS1-Sl for State and Local Government Agencies*. Tallahassee, FL: Florida Department of State, 2013.

StateMaster. “Transportation Statistics: Toll Road Mileage (Most Recent) by State.” Accessed November 22, 2015. http://www.StateMaster.com/graph/trn_tol_roa_mil-transportation-toll-road-mileage.

Thierer, Adam. “Techno-Panic Cycles (and How the Latest Privacy Scare Fits in).” Technology Liberation Front. February 24, 2011. http://techliberation.com/2011/02/24/techno-panic-cycles-andhow-the-latest-privacy-scare-fits-in.

Turk, M. A. and A. P. Pentland. “Face Recognition Using Eigenfaces.” In *Proceedings of IEEE Computer Society Conference on Computer Vision and Pattern Recognition ‘91*. doi 10.1109/CVPR.1991.139758.

VinTech. “Top 5 Cities with the Largest Surveillance Camera Networks.” May 4, 2011. http://www.vintechnology.com/journal/uncategorized/top-5-cities-with-the-largest-surveillance-camera-networks/.

Vorder Bruegge, Richard W. “Facial Recognition and Identification Initiatives.” FBI. 2010. http://biometrics.org/bc2010/presentations/DOJ/vorder_bruegge-Facial-Recognition-and-Identification-Initiatives.pdf.

Watson, Jim. “NYPD Uses Facebook and Facial Recognition Program to Arrest Suspect.” RT. March 19, 2012, https://www.rt.com/usa/new-york-barbershop-shooting-951/.

Woodward, John D. *Biometrics: Facing up to Terrorism*. Santa Monica, CA: RAND, 2001.

Zurawski, Nils. “I Know Where You Live! Aspects of Watching, Surveillance and Social Control in a Conflict Zone. “*Surveillance & Society* (2005): 508.

THIS PAGE INTENTIONALLY LEFT BLANK

INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center
   Ft. Belvoir, Virginia

2. Dudley Knox Library
   Naval Postgraduate School
   Monterey, California